Journal of Process Control 24 (2014) 621–639

Contents lists available at ScienceDirect

Journal of Process Control

journal homepage: www.elsevier.com/locate/jprocont

Experimental validation of a resilient monitoring and control system

Wen-Chiao Lin[a,1], Kris R.E. Villez[b], Humberto E. Garcia[a,*]

[a] Dynamic Systems Integration, Optimization, and Resilient Controls Group, Idaho National Laboratory, Idaho Falls, ID 83415-3570, USA
[b] Eawag Process Engineering, Überlandstrasse 133, P.O. Box 611, 8600 Dübendorf, Switzerland

ARTICLE INFO

Article history:
Received 24 October 2013
Received in revised form 7 March 2014
Accepted 7 March 2014
Available online 26 April 2014

Keywords:
Resilient monitoring and control systems
Experimental validation
Cyber-physical attacks
Health condition assessment
Hardware-in-the-loop
Adaptive supervisory controls
Fault detection
Identification
Accommodation

ABSTRACT

Complex, high performance, engineering systems have to be closely monitored and controlled to ensure safe operation and protect public from potential hazards. One of the main challenges in designing monitoring and control algorithms for these systems is that sensors and actuators may be malfunctioning due to malicious or natural causes. To address this challenge, this paper addresses a resilient monitoring and control (ReMAC) system by expanding previously developed resilient condition assessment monitoring systems and Kalman filter-based diagnostic methods and integrating them with a supervisory controller developed here. While the monitoring and diagnostic algorithms assess plant cyber and physical health conditions, the supervisory controller selects, from a set of candidates, the best controller based on the current plant health assessments. To experimentally demonstrate its enhanced performance, the developed ReMAC system is then used for monitoring and control of a chemical reactor with a water cooling system in a hardware-in-the-loop setting, where the reactor is computer simulated and the water cooling system is implemented by a machine condition monitoring testbed at Idaho National Laboratory. Results show that the ReMAC system is able to make correct plant health assessments despite sensor malfunctioning due to cyber attacks and make decisions that achieve best control actions despite possible actuator malfunctioning. Monitoring challenges caused by mismatches between assumed system component models and actual measurements are also identified for future work.

Published by Elsevier Ltd.

1. Introduction

1.1. Motivation

Complex high performance systems, such as chemical production plants, refineries, and power generation and transportation systems have to be closely *monitored* and *controlled* to ensure safe operation and protect the public from potential hazards. One of the main challenges in designing monitoring and control algorithms for these systems is that sensors and actuators may be malfunctioning due to natural or malicious causes. For example, if the monitoring system is connected to the some information network, false data may be injected to sensor measurements via cyber attacks. Likewise, valves regulating fluid flows in a cooling system may be stuck due to accumulation of deposits, corrosion, or other forms of wear-and-tear. This paper aims to develop a resilient monitoring and control (ReMAC) system, whose performance degrades gracefully under natural or malicious malfunctioning of sensors and actuators. In particular, we expand previously developed resilient condition assessment monitoring systems [1] and Kalman filter-based diagnosis algorithms [2] and integrate them with a supervisory control mechanism developed here. While the monitoring and diagnostic algorithms assess plant (cyber and physical) health conditions, the supervisory controller selects, from a set of candidates, the best controller based on these health assessments. The developed ReMAC system is then experimentally demonstrated on a chemical reactor with a water cooling system in a hardware-in-the-loop (HiL) setting, where the reactor is computer simulated and the water cooling system is implemented by a machine condition monitoring (MCM) testbed at Idaho National Laboratory (INL).

1.2. Review of related work

Research on resilient systems is a relatively new subject and recent work on resilient systems can be found in [3–14,1,15–19,2]. In particular, [3] provides collections of papers that treat resilience engineering as a paradigm for safety management that focuses on “how to help people cope with complexity under pressure to achieve success.” These papers explore different facets of resilience as “the ability to anticipate and adapt to the potential for surprise and failure.” Based on these work, [5] further identifies four

[*] Corresponding author. Tel.: +1 2085267769; fax: +1 2085263150.
[1] W.-C. Lin has moved to General Motors Company.

http://dx.doi.org/10.1016/j.jprocont.2014.03.006
0959-1524/Published by Elsevier Ltd.

cornerstones of resilience as knowing "what to do," "what to look for," "what to expect," and "what has happened."

Relations between resilience and robustness have been investigated. For example, [6] addresses different fire-prone ecological systems and suggests that robustness tradeoffs in these systems demonstrate resilience. In [7], resilient control systems that emphasize control design in an adversarial and uncertain cyber environment (as opposed to physical disturbances) are developed. This control design is viewed as pivoting on the tradeoff between robustness and resilience. Optimality criteria are proposed for tradeoff between robustness and resilience in modern industrial control systems.

Further developments of resilient systems with uncertain cyber environments can be found in [8,9]. Specifically, [8] provides a conceptual framework and brief overview of the architectural considerations for designing systems that operate in hostile cyber environment with uncertainties in complex networks and human interactions. The work in [9] develops an intelligent resilient control algorithm for a wireless networked control system based on quantification of the concept of resiliency in terms of quality of control. Here, resiliency maintains normal operations in the face of wireless interference incidents. Ref. [10] further uses the quality of control for designing resilient control strategies for model-based building control, improving building automation systems.

Resilient systems have also been considered regarding security issues in, for example, [11,12]. While [11] describes experiences and success in cyber security programs leading to more robust, secure, and resilient monitoring and control systems in industrial assets, [12] discusses security-related definitions for resilience, which includes integrity and confidentiality in addition to availability.

Developments of resilient systems for computer systems and for monitoring critical infrastructures can be found, for instance, in [13,14]. In particular, in [13], metadata-based resilience policies are enforced to design computing systems that can dynamically adapt in a predictable way to unexpected events. In [14], basic paradigms are proposed for integration of diverse fault detection and identification methods and control methods for achieving resilience in critical infrastructures.

This work builds on the resilient monitoring systems developed in [4,1,15–19] and Kalman filter-based diagnosis methods in [2]. In [4,1], it is assumed that a set of sensors observing process variables are deployed throughout a monitored plant, which is subject to process disturbances (e.g., unplanned, random process anomalies and deliberate, non-random physical attacks). Likewise, the sensors are subject to disturbances (e.g., unplanned, random sensor faults and failures and cyber-attacks), which cause them to project false data/observations. Although [4] and [1] developed similar monitoring architectures, the design approaches for the components are different. In particular, the monitoring system designed in [1] aims at selecting sensors to make plant health assessments within desired time periods despite cyber attacks, while that in [4] focuses on selecting sensor configurations to maximize plant health assessment confidence. Moreover, some advantages are also afforded by the approach considered in [1], such as faster computations of the monitored plant assessments. Following this line of work, [15] developed an active probing method for sensor data quality assessment. Integration of the active probing method into the resilient monitoring structure is documented in [16], while [17,18] consider application of the developed monitoring system to simplified power plants consisting of a boiler and a turbine. Reference [19], extending the work in [1], developed game-theoretic formulations for resilient monitoring systems that improve monitoring performance when natural or malicious sensor malfunctioning is incorrectly characterized.

The Kalman-filter based fault detection identification (FDI) method as applied here was first presented in [2]. In essence, this method is based on the key observation that the expected values of one-step ahead prediction residuals obtained by means of the Kalman filter are unique for fault type (e.g., bias, drift), fault location (affected actuator, process or sensor), and magnitude (e.g., bias magnitude). To obtain high sensitivity and specificity, the method requires that a reliable model is available. Alternative diagnostic methods are available when this is a challenging requirement, either based on data mining tools (e.g., [20] or on course-grained system and/or data representations (e.g., [21,22]).

This paper integrates the work in [1,2] with a supervisory control algorithm for developing a resilient monitoring and control algorithm. Note that, while the work in [1] aims at assessing the overall monitored plant conditions, the algorithms in [2] determine the health of monitored plant components. Hence, in the following, we will refer to methods in [1,2] as systems- and component-centric, respectively.

1.3. Main contributions and organization of paper

The main contributions of this paper include the following.

- Development of a resilient monitoring and control (ReMAC) system that combines previously developed systems- and component-centric monitoring algorithms [1,2] with supervisory control methods.
- Application of the developed ReMAC system to a chemical reactor with a water cooling system in an HiL setting, where the reactor is computer simulated and the water cooling system is implemented by an MCM testbed at INL.

As this paper is on experimental verification of the developed algorithms, we focus more on describing the background knowledge, experimental setups, scenarios considered, and simulation results. Whenever appropriate, references are given for readers who wish to read the theory and analysis in more detail. The rest of this paper is organized as follows. Section 2 introduces the overall architecture of the developed ReMAC system, while Section 3 describes the algorithms implementing constituent components of it. The monitored plant considered is detailed in Section 4. Implementation of the ReMAC system for the monitored plant considered and simulation results are given in Sections 5 and 6, respectively. Finally, Section 7 concludes the paper and describes future work.

2. Monitoring architecture

This section describes the architecture of the developed resilient monitoring and control (ReMAC) system, shown in Fig. 1.

In particular, we consider a monitored plant, which is subject to physical disturbances (e.g., process anomalies). A set of sensors are deployed to observe the plant process variables, while a set of regulatory controllers regulate the plant via actuators. The sensors and actuators are subject to natural or malicious disturbances, such as cyber attacks (e.g., injecting false data to the sensors) or physical disturbances (e.g., decreased efficiency due to aging in a pump). In view of sensor disturbances, a scalar, referred to as the data quality (DQ), is dynamically assigned to quantify the trustworthiness of its reported measurement. While recent work has developed active methodologies for assigning sensor DQs [15–17], this paper does not address this particular element. Instead, the monitoring systems considered in this work assume that sensor DQs are computed by a watch dog system, which assign sensor data qualities based on, e.g., cyber attack assessments, sensor data traffic, or state estimation comparisons. The sensor signals are used in a Kalman

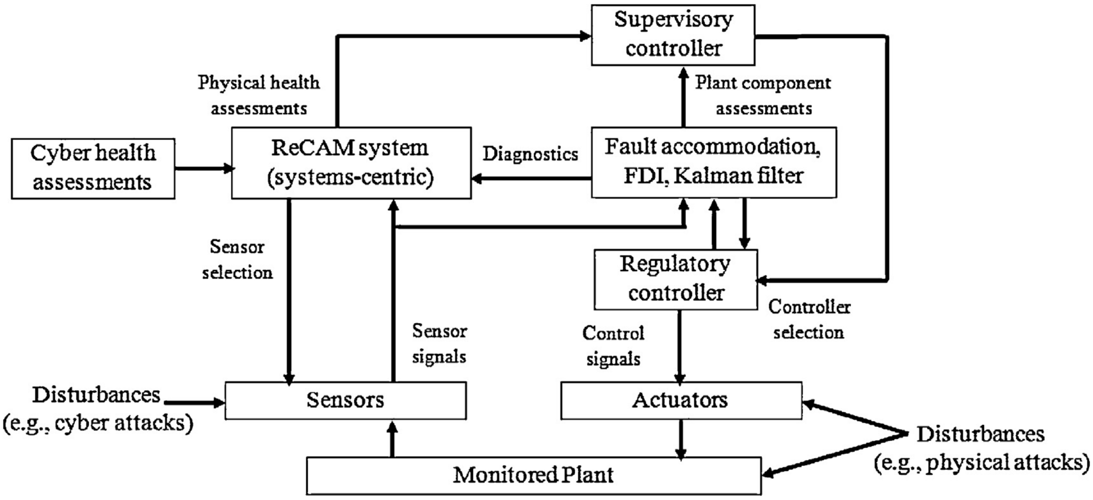

Supervisory controller
Physical health assessments
Plant component assessments
Cyber health assessments
ReCAM system (systems-centric)
Diagnostics
Fault accommodation, FDI, Kalman filter
Sensor selection
Regulatory controller
Sensor signals
Control signals
Controller selection
Disturbances (e.g., cyber attacks)
Sensors
Actuators
Disturbances (e.g., physical attacks)
Monitored Plant

Fig. 1. Architecture of ReMAC.

filter-based (component-centric) diagnosis algorithm to assess the health of the monitored plant components (including the actuators). This diagnosis algorithm consists of a set of three modules: (1) fault accommodation; (2) fault detection and identification (FDI); and (3) a Kalman filter, which requires, in addition to sensor signals, control signals in the regulatory controllers. Likewise, the systems-centric resilient condition assessment monitoring (ReCAM) system uses sensor signals along with their DQs and diagnosis results from Kalman filter-based methods to assess the overall plant health. In addition, the ReCAM system dynamically selects sensor configurations to improve its monitoring results. The sensor selections provide features such as avoiding using sensors with low data qualities and, hence, improving monitoring performance. The systems and component-centric assessments are in turn used by a supervisory controller to select the best controllers from a set of candidate regulatory controllers, which utilize state estimate results from the Kalman filter. The controller selection provide the ability to apply appropriate actions given assessed plant conditions (e.g., maximize cooling water flow rate to avoid system overheating) or avoid using controllers that use actuators that are assessed to be faulty. In the following sections, we give a brief overview of the main components in this architecture and describe them in more detail in Section 3.

2.1. Kalman filter-based (component-centric) diagnosis methods

The Kalman filter-based (component-centric) diagnosis methods consist of a Kalman filter, an FDI module, and a fault accommodation module. The Kalman filter is used to

(1) deliver state estimates to the regulatory controllers which are part of the feedback section, and
(2) deliver prediction errors to the FDI module.

The FDI module is used to detect and identify faults and failures in system components. The fault accommodation module is used to correct faulty state estimates and data. This is necessary to enable detection and identification of multiple faults in series.

The Kalman filter-based diagnosis methods are used for identifying failures of particular components with the advantage that they react faster but prone to mistakes if sensor data are inaccurate. Hence, in the event of confirmed incorrect diagnostics after inspection, reset is implemented to re-start the diagnostic calculations.

2.2. ReCAM (systems-centric) methods

The ReCAM system considered is modified from that developed in [1], which include three functional layers: process variable assessment, physical health assessment, and sensor adaptation. A ReCAM system consumes two elements, namely, sensor and DQ data, and produces two elements, namely, physical health assessment and sensor configuration data. Thus, observations from a selected set of sensors along with their corresponding DQs are used in the process variable assessment layer to estimate process variable values, which are in turn used in the plant assessment layer to assess the plant health conditions. The sensor adaptation layer then dynamically selects the set of sensors for subsequent observations so as to improve the monitoring performance.

ReCAM system methods are used for assessing overall health of the monitored plant with the characteristic of being resilient to sensor failures but typically takes a long time to make definite plant assessments.

2.3. Supervisory control

Controllers are used in the monitored plant for regulating various processes. Considering possible physical anomalies in the monitored plant, a set of candidate controllers are designed, each using a different set of actuators and may have different control objectives. Based on the assesses condition of the monitored system from ReMAC system and Kalman filter-based methods, a supervisory controller selects the best controller from this set considering the health of the actuators and the overall plant. For example, if a certain actuator is determined to be malfunctioning, the supervisory controller will then select a controller that does not use this actuator. Likewise, if the monitored plant is assessed to be overheating, a controller that introduces maximum water flow to cool the system will be selected. In this work, an automaton is used to design the supervisory controller. Fig. 2 illustrates such an automaton, where each state corresponds to a particular regulatory considered.

State transitions occur when assessments, such as malfunctioning of an actuator, is made. For example, during initial operations, where the monitored system is normal, the automaton is in state 0, selecting a controller that suffices in normal operating conditions. However, when an assessment is made that a certain part of the plant is overheating, a state transition is made so that a controller that introduces maximum cooling (e.g., maximum cooling water

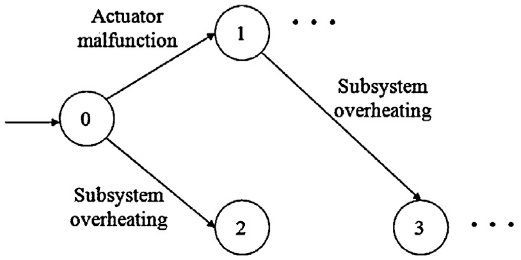


Fig. 2. Concept of supervisory controller.

flow) is used. Although Fig. 2 shows a relatively simple automaton, more complex automata, including directed cycles, are permitted.

3. ReMAC system components

In this section, algorithms implementing components of the ReMAC system architecture in Section 2 are developed. In particular, the Kalman filter-based (component-centric) diagnosis and ReCAM (systems-centric) methods are described. As the candidate regulatory and supervisory controllers are strongly tied to the monitored plant considered, detailed description of them are given in Section 4.3 after description of the monitored plant.

3.1. *Kalman filter-based (component-centric) diagnosis methods*

Fig. 3 gives an overview of modules (i.e., fault accommodation, Kalman filter, FDI) implementing the Kalman filter-based diagnosis method and their coupling to neighboring modules.

Raw data from the sensors and the regulatory controllers (current control actions are routed to fault accommodation, where the data is corrected for the current set of identified faults (e.g. bias/drift in sensor, stuck valve). The corrected data enters the Kalman filter module which delivers (1) state estimates, to be sent to the regulatory controllers, and (2) prediction residuals, which are sent to the FDI module. This FDI module delivers to fault accommodation the identified faults and corrections (location, type and magnitude of fault) based on prediction residuals and corrected data (for previously identified faults). The resulting accumulated set of fault data are sent to the supervisory controller. The likelihood for each combination of location and type of fault is sent to the ReCAM system.

3.1.1. *Fault accommodation*

The considered faults fall in two classes. The first one consists of additive faults such as bias and drift of either actuators (e.g., valves) or sensors (e.g., valve position measurements). The second consists of non-additive faults. In this work, this is limited to stuck (non-responsive) valves. Fault accommodation for additive faults consists of subtracting identified bias or accumulated drift from the actuator and sensor signals. In the case of a stuck valve, one modifies the actuator signal so that it matches the position at which the valve is estimated to be. In both cases, the required information (bias/drift parameter or stuck valve position) is delivered by the Kalman filter driven FDI scheme as discussed below.

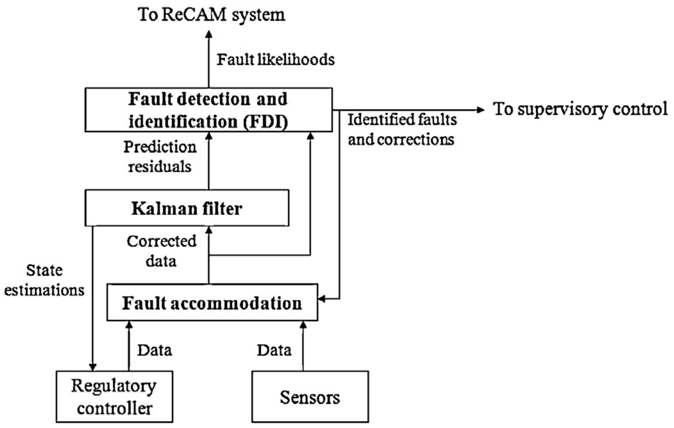


Fig. 3. Kalman-based (component centric) modules.

3.1.2. *Kalman filter*

Kalman filtering is usually applied for a fixed-step discrete time state-space model:

$$x(k) = Ax(k-1) + Bu(k-1) + Fv(k) \tag{3.1}$$

$$y(k) = Cx(k) + Du(k) + Gw(k), \tag{3.2}$$

where $v(k)$ and $w(k)$ are independently and identically distributed (i.i.d.) zero-mean white noise vectors. In this case, optimal state estimates, x_s, are obtained through prediction and updating steps:

$$x_p(k) = Ax_s(k-1) + Bu(k-1) \quad \text{(predict)} \tag{3.3}$$

$$x_s(k) = x_s(k) - Ky(k) \quad \text{(update)}. \tag{3.4}$$

As long as the matrices A, B, C, D, F and G remain the same (time-invariant), the Kalman gain will converge exponentially fast to a steady-state form. Quite often, this facilitates implementation as one can compute this steady-state Kalman gain a priori and use it instead of the continuously updated Kalman gain matrix, thereby avoiding online execution of matrix inversions to update this matrix. Note that the Kalman filter is a well-known mathematical device for on-line state estimation, sometimes referred to as soft-sensing [23]. It is optimal for linear time-invariant systems in the maximum likelihood sense, which explains part of its popularity. When the underlying assumptions are not met, the Kalman filter corresponds to the best linear unbiased estimator for the process states. Fast-computing alternatives designed for use with nonlinear systems include the extended Kalman filter (EKF) [23] and the unscented Kalman filter (UKF) [24]. A crucial requirement is the availability of a reasonably reliable model.

3.1.3. *Fault detection and identification (FDI)*

The fault detection and identification module consists of three tools described in the next paragraphs.

(1) Kalman filter: This module is driven by residuals produced by the Kalman filter. These residuals consists of the difference between measurement predictions and actual measurements. Such residuals are known to exhibit predictable profiles under given fault scenarios, i.e. when fault type (bias, drift), fault location (which actuator, sensor) and time of fault introduction are known. This feature is exploited in several publications to suggest the most likely fault scenario. The method of [2], which adds drift as an additive fault as well as non-additive faults, such as sticky behavior and non-responsiveness (stuck), to the library of faults, is used in this work.

(2) Principal component analysis (PCA): PCA [25] is based on the following linear model:

$$X = T \cdot P' + E, \tag{3.5}$$

where the original data, X, is approximated by the principal components, P, and corresponding scores, T. The term E is the set of residuals. The PCA model is usually estimated in the least-squares (LS) sense. This corresponds to maximum likelihood (ML) estimation in particular instances of this problem. This can be achieved through singular value decomposition (SVD). This classic approach requires that the data (X-matrix) is complete. If some data is missing, PCA needs to be estimated differently. This can still be done in the LS/ML sense, though another algorithm is required. Most promising is the EM (expectation–maximization) algorithm [26,27]. With this algorithm, one alternates between a step which estimates the scores (*T*, expectation) and a step which estimates the components (*P*, maximization). The EM algorithm is proven to converge to the global optimum and will be used for PCA estimation with missing data. Once established, the PCA model components, *P*, are fixed. Thus, for on-line application only the scores, *T*, are required. Subject to missing data, it may or may not be possible to compute these scores. This is possible if $(Px' \cdot Px)$ is non-empty and full rank, with *Px* being the rows of the component matrix corresponding to the measured data [28]. This condition can be evaluated on-line. If the scores can be computed, then the PCA tool works as normal.

(3) Trend analysis: The applied trend analysis method is based on the fitting of piece-wise polynomials based on an interval-halving method [29]. The method has been implemented for univariate time series with observations at fixed intervals. However, the method poses no mathematical challenges to handle data at changing intervals. Changes in the implementation are largely of practical nature. In particular, the interval-halving based method should be presented with the time stamps of the given observations rather than assuming fixed, preset time intervals. The above method was selected for its relative simplicity. Alternative algorithms are available or under development (e.g., [2,22]).

Of the above tools, the first and third are expected to work continuously. More precisely, both of these tools require a window of data which will be set to a large enough value so that it can be guaranteed that sufficient measurements for these tools are present. The second tool works only conditionally, because of the invertibility requirement, which cannot necessarily be satisfied by extending the time window.

The supervisory control requires however that a particular fault condition is selected as the most probable one. This is done as soon as the ratio of the largest likelihood to the second largest likelihood is larger than a user specified number (e.g., 5). For fault accommodation, the parameters identified by means of the Kalman filter module are used. This selection was made based on experimental evidence showing that the estimates by other modules are not as reliable.

3.2. ReCAM (systems-centric) methods

We first give an overview of the ReCAM system, with Sections 3.2.1–3.2.4 providing more explanations. Fig. 4 illustrates the developed ReCAM structure, which consists of three layers: process variable assessment, plant or physical health assessment, and sensor adaptation.

In this structure, sensors constituting a sensor network are deployed throughout a monitored plant, which may be subject to physical process disturbances. Likewise, sensors may also be subject to disturbances, such as cyber-attacks, and trustworthiness of their data are quantified by sensor DQs. Operation of these three layers are briefly described next.

In the process variable assessment layer, observation data and associated DQs for a selected sensor configuration are used to calculate process variable (PV) probability distributions. While several other rules (such as the cautious rule of combination in [30]) may be considered, these calculations are combined based on Dempster–Shafer rule [31] if more than one sensor is active in

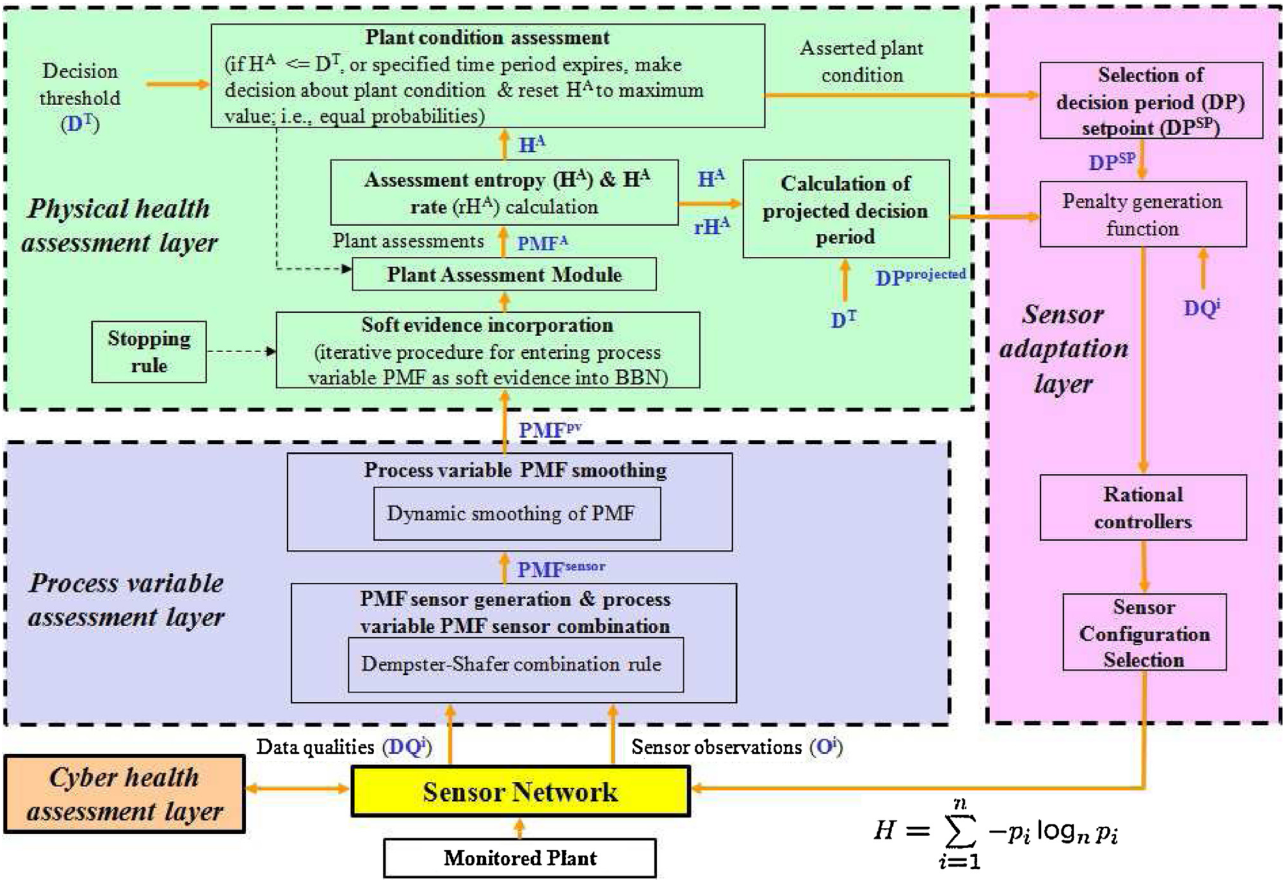

Decision threshold (D^T)
Plant condition assessment
(if $H^A <= D^T$, or specified time period expires, make decision about plant condition & reset H^A to maximum value; i.e., equal probabilities)
Asserted plant condition
Selection of decision period (DP) setpoint (DP^{SP})
DP^{SP}
Penalty generation function
H^A
Assessment entropy (H^A) & H^A rate (rH^A) calculation
H^A
rH^A
Calculation of projected decision period
Physical health assessment layer
Plant assessments
PMF^A
Plant Assessment Module
$DP^{projected}$
D^T
DQ^i
Sensor adaptation layer
Stopping rule
Soft evidence incorporation
(iterative procedure for entering process variable PMF as soft evidence into BBN)
PMF^{pv}
Process variable PMF smoothing
Dynamic smoothing of PMF
Rational controllers
PMF^{sensor}
Process variable assessment layer
PMF sensor generation & process variable PMF sensor combination
Dempster-Shafer combination rule
Sensor Configuration Selection
Data qualities (DQ^i)
Sensor observations (O^i)
Cyber health assessment layer
Sensor Network
Monitored Plant
$H = \sum_{i=1}^{n} -p_i \log_n p_i$

Fig. 4. Mathematical structure of ReCAM system.

observing a particular process variable. To prevent abrupt changes to PV estimations, calculated PV probability distributions are then fed as inputs to a smoothing process to estimate PV probability distributions. The estimated PV probability distributions are then used as evidence in the plant or physical health assessment layer to assess the condition of the plant by calculating probability distribution of the plant state. Since the plant is subject to process disturbances and, hence, process variables are influenced by the state of the plant probabilistically, these calculations are based on probabilistic reasoning methods. In particular, Bayesian belief networks (BBN) are used in this work. The BBN is used repeatedly, with prior probabilities set as the updated plant assessments from the previous time instant. The entropy (indicating the confidence) of the plant assessment probability distribution is subsequently calculated. This entropy is similar to the notion of information entropy in communication systems [32]. If this plant assessment entropy is lower than a user defined threshold (indicating required confidence on plant assessments), a definite decision on the plant status is made and reported to the plant operator based on the computed plant assessment probability distribution; then the plant assessment process repeats (with prior probabilities of roots in the BBN set to complete ignorance, i.e., uniform distributions). If the plant assessment entropy is not lower than the specified threshold, a predicted decision period, which is an estimated time between the last and next definite decision of the plant status, is computed. Based on the difference between the predicted and desired decision periods, penalties are accordingly generated for the rational controllers to select sensor configurations for subsequent computation in the process variable assessment layer. We refer the reader to [1] for a complete description of this ReCAM system.

3.2.1. Monitored plant and sensors

In this section, models of the monitored plant and sensor measurements of PVs are introduced. Specifically, let V_i, $i = 1, 2, \ldots, M$, denote random variables of M process variables. These random variables are assumed to take on discrete values, e.g., low, normal, or high. Likewise, let G denote a random variable describing plant state, which also take on discrete values, e.g., normal, degrading, or down. The monitored plant is modeled as a set of conditional probabilities:

$$\begin{cases} [P(V_i|G)] & \text{for } i \in I_1 \subseteq \{1, 2, \ldots, M\}, \\ [P(V_i|V_j, G)] & \text{for } i \in I_2 \subseteq \{1, 2, \ldots, M\}, \\ [P(V_i|V_j)] & \text{for some pairs } i, j \in \{1, 2, \ldots, M\}. \end{cases} \tag{3.6}$$

To model cyber attacks, a bias is accordingly added to the sensor measurement y_m based on the assumed severity/threat level of a given attack as follows:

$$y_r = \begin{cases} y_m & \text{if sensor is not attacked} \\ y_m + b & \text{if sensor is attacked,} \end{cases} \tag{3.7}$$

where y_r is the reported sensor observation, y_m is the sensor measurement, and b is the bias added by the cyber attack. This type of attack, commonly referred to in the literature as integrity attacks, is similar to the additive attacks described in [33]. Notice also that, without loss of generality, we only consider integrity attacks (i.e., sensor measurements are maliciously changed as in (3.7)) in this paper. Sensor outputs are then computed by discretizing measured process values into discrete quantities such as low, normal, and high. A DQ model is used to characterize the effect of attacks on the quality of sensor measurements.

3.2.2. Process variable assessment layer

Consider a given PV, V, observed by a set of sensors S_i, $i = 1, 2, \ldots$ with associated DQs, denoted by DQ_i. The goal in this layer is to estimate the probability mass function (PMF) of V given the sensor measurements and DQs at measurement times $k = 1, 2, \ldots$. Suppose, at time k, the DQ of sensor S_i is DQ_i and that S_i observes $\sigma \in \Sigma$, where Σ is the set of states of V (e.g., low (L), normal (N), or high (H)). The notion of *believability* of a sensor is employed to interpret this observation in the form of PMF for V [4]. Formally, *believability* is defined as follows:

$$B_i = \frac{1}{|\Sigma|}[(|\Sigma| - 1)DQ_i + 1], \tag{3.8}$$

where $|\Sigma|$ denotes the cardinality of the process variable state space, Σ (i.e., $|\Sigma|$ denotes the number of states in Σ). Based on B_i, we calculate a target PMF_i^* as input to the smoothing process mentioned below, where $PMF_i^*(\sigma)$ denotes the probability of $V = \sigma$. In particular, based on the observation s of S_i, PMF_i^* is given by:

$$PMF_i^*(\delta) = P\{V = \delta | s = \sigma\} = \begin{cases} B_i & \text{if } \delta = \sigma, \\ \dfrac{1 - B_i}{|\Sigma| - 1} & \text{if } \delta \neq \sigma. \end{cases} \tag{3.9}$$

Note that the calculation of PMF_i^* above results from only one measurement reported by S_i. If there are multiple (active) sensors observing V, the Dempster–Shafer combination rule [31] is used to combine the target PMFs calculated for each sensor (see [1] for detailed mathematical equations). To prevent abrupt changes in the estimations of V, the combined target PMF is used as an input to a smoothing process, whose output is the estimated PMF of V, denoted by $\hat{P}(V)$. An example of the smoothing process is a first order filter as follows:

$$\tau \frac{d}{dt} PMF(t) = PMF^*(k) - PMF(t), \tag{3.10}$$

where

- $PMF^*(k)$ is the (combined) target PMF calculated at measurement time k;
- at time instant k, dynamics are simulated with target $PMF^*(k)$ from t_{k-1} to $t_k = t_{k-1} + \Delta t$, where $t_0 = 0$;
- Δt and τ are tuning parameters;
- $PMF(t_k)$ is $\hat{P}(V)$ at time k;

Moreover, if there is not any sensor active for V at $k - 1$, i.e., $PMF(t_{k-1})$ does not exist, we set $PMF(t_{k-1})$ as the PMF of V calculated based on the plant PMF assessments at time $k - 1$ (to be described in Section 3.2.3) and the plant model (3.6).

3.2.3. Plant assessment layer

The plant assessment layer assesses the plant conditions based on the estimated process variable PMFs calculated at each time k. While numerous probabilistic reasoning methods may be used for this purpose, the plant assessment module utilizes a BBN in the present work as an example, where estimated PMFs, as opposed to deterministic observations, are entered using a modification of the iterative proportional fitting procedure (IPFP) documented in [34]. The plant assessment algorithm is repeatedly applied as $\hat{P}(V_i)$, $i = 1, 2, \ldots, M$ are calculated from sensor measurements sequentially collected at time $k = 1, 2, \ldots$. When using the plant assessment algorithm to compute the a posteriori belief of plant state $\hat{P}(G)$, the initial (a priori) belief of plant state is the result from the plant assessment computed at previous time step. That is, if the current time index is k, the a priori belief for the plant assessment algorithm is $\hat{P}(G)$ calculated at time $k - 1$. When $\hat{P}(V_i)$, $i = 1, 2, \ldots, M$ at time k are consistent with $\hat{P}(G)$ calculated at time $k - 1$, the entropy of the plant assessment, defined as:

$$H^A = \sum_{\sigma \in \Sigma_G} -\hat{P}(G = \sigma)\log_{|\Sigma_G|}\hat{P}(G = \sigma), \tag{3.11}$$

decreases from its previous value calculated at $k-1$. Once the entropy of plant health assessments decreases below a (user-defined) decision threshold, a definite decision is made about the plant state (e.g., whether the plant is normal, degrading, or down). This belief, along with the current plant assessment PMF, $\hat{P}(G)$, are reported to the plant operator. The belief of plant state is then reset to complete ignorance for the subsequent assessment, and the plant assessment procedure repeats. Resetting here means resetting the roots of the BBN. The notion of decision period is of importance. It is defined as the time window that starts at the moment of resetting the belief of plant state to complete ignorance and ends when a decision on plant state is made. Decision period is the time needed to make a definite decision regarding the state of the monitored plant.

Because conditional probability tables (CPTs) of BBNs are trained assuming perfect DQs, they need to be accordingly modified considering the estimated DQs. Due to space limitations, we refer to [1] for a detailed description of the CPT modification.

3.2.4. Sensor adaptation algorithm

The goal of the sensor adaptation layer is to meet a certain (user-defined) decision period. Consequently, it is not to find an optimal sensor configuration (SC) per se, but rather to control selections of SCs so that the entropy of plant assessments decreases as needed to meet the decision period requirement. Note then that under the proposed recursive strategy, there is no need for plant operating conditions and sensor DQs to stay the same, but they can change. Sensor adaptation is based on theory of rational behavior (TRB) [35], with each sensor being equipped with a rational controller (RC) to select its operation mode. RCs are designed to achieve monitoring objectives based on penalties received.

RCs designed here are based on the ring element [35], with state space [0, 1). When the ring element is in [0, 0.5), the sensor associated with it is inactive, thus reporting no data. Similarly, when the ring element is in [0.5, 1), the sensor associated with it is active thus reporting its measurement. The dynamics of the ring element is described as follows:

$$\dot{x} = \varphi^N(\{x\}) \tag{3.12}$$

where $\{x\}$ takes the fractional part of x, $\varphi(x)$ is the penalty associated with x, and N is a positive number referred to as the measure of rationality. The dynamics in (3.12) is approximated as

$$x(k+1) = x(k) + \Delta t \varphi^N(\{x(k)\}) \tag{3.13}$$

where k denoted the index of the measurement step and $\Delta t = 0.001$ in this work.

Ring elements are penalized so that the desired decision period is achieved within some tolerance. To this end, the expected decision period is estimated based on the time elapsed since last decision and the current rate of assessment entropy change. Due to space limitations, we refer to [1] for a detailed description of the penalty functions.

3.3. Integration of systems and component-centric methods

In this section, we discuss modifications of the methods described in Sections 3.1 and 3.2 for integration into a ReMAC system. There are two main considerations. The first consideration is that diagnosis results made by Kalman filter-based (component centric) diagnosis methods are used in the ReCAM system for assessing the overall plant health. The ReCAM system is hence slightly modified to take diagnosed component health as a input. Although the algorithms developed here are not restricted to a single fault, we first consider the case that the Kalman filter-based method is designed to assess the health of one component and that possible states of the component is "normal," "degrading," and "down." Then the input to the ReCAM system is the assessed probability of each of these states calculated by the Kalman filter-based methods. To accommodate for this, the process variable assessment and plant assessment layers are modified. First consider the process variable assessment layer. Whenever the input from Kalman filter-based calculations becomes available, say at time k, we consider an additional process variable, $V_{additional}$, with probability distribution estimate, $\hat{P}(V_{additional})$, calculated by (3.10) using the input as $PMF^*(k)$. In the plant assessment layer, the BBN considered for the ReCAM system will have one additional node, indicating the calculated health of the considered component. This node is similar to other nodes with a CPT characterizing casual relations with its parents and is also modified considering the DQ of the sensor that was used to calculate the health of the component. Similar to the other process variables, $\hat{P}(V_{additional})$, is then entered as evidence for the additional node. Extension to more than one component healths input is obvious (for each additional component, we consider one additional process variable and add one node to the BBN).

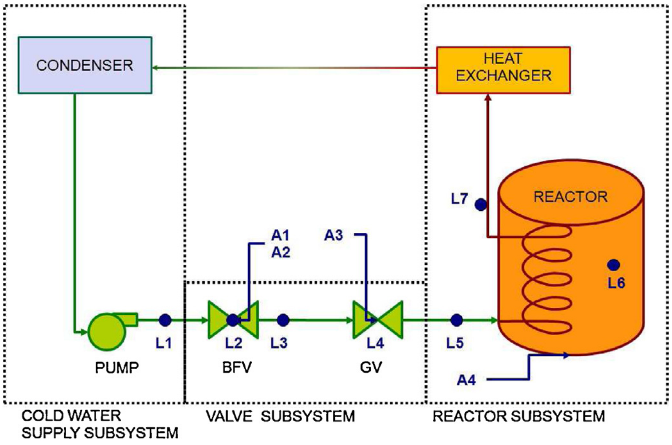


Fig. 5. Monitored plant considered.

The second consideration is that the ReCAM system changes the sensor configuration dynamically. However, the Kalman filter-based diagnosis methods were developed assuming fixed sensor configurations. Hence, these methods have to be modified to accommodate for dynamically changing sensor configurations. In particular, the observation Eq. (3.2) changes at every time instant. This means that the Kalman gain also needs to be recomputed at each time instant. Furthermore, this may mean, under extreme circumstances, that the residual profiles associated with different fault scenarios may not be substantially different anymore (e.g. because a key symptom appears in a sensor who is infrequently sampled). In such cases, particular attention should be given to the idea that several alternative fault conditions can explain the available information, which in this case is available in the form of prediction residuals.

4. Monitored plant considered

To obtain a realistic, real-life validation of the developed ReMAC system, a plant consisting of both physical and simulated elements was considered within an HiL experimental setting. In what follows, an overview of the monitored system is given first. Then, its constituting components as well as deployed sensor and actuators are described in detail. Finally, the regulatory and supervisory controllers are also described.

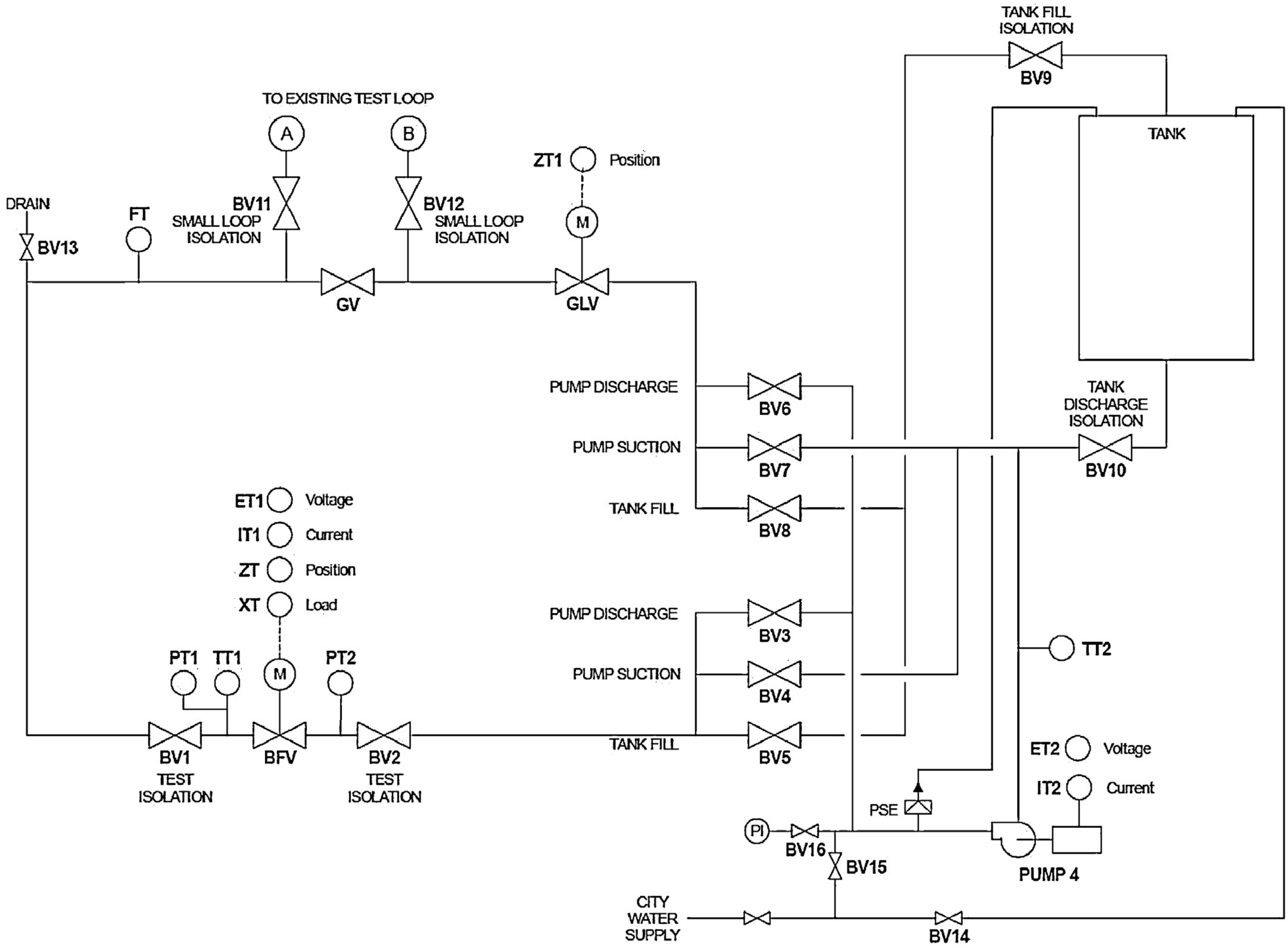


Fig. 6. Scheme of the INL MCM testbed.

4.1. *Overview of monitored plant*

Fig. 5 shows a schematic overview of the considered monitored plant. The goal of the plant is to provide proper cooling to a chemical reactor plant.

Three subsystems are indicated in Fig. 5. The first subsystem (left) is the cold water supply subsystem, which consists of a cold water source (condenser) and a pump. The second subsystem (middle) is called the valve subsystem, which includes two valves, a butterfly valve (BFV) and a glove valve (GV). Finally, the third subsystem (right) is called the Reactor Subsystem, which consists of an exothermic reactor with a heat exchanging coil and a hot water sink (heat exchanger). The hot cooling water is sent back from the heat exchanger to the condenser to provide cold water. Also indicated in the figure are seven locations Li, $i = 1, 2, \ldots, 7$, indicating places where sensors and actuators are installed. The labels, Ai, $i = 1, 2, 3, 4$, indicate four actuator signals, which, along with the sensors, are further specified in Section 4.1.4.

4.1.1. *Cold water supply subsystem*

The cold water supply subsystem consists of a cold water source (condenser), a pump, and connecting tubing. This part of the system is realized through the MCM test bed at INL. Fig. 6 shows a scheme of the INL MCM test bed.

The water reservoir (TANK) of the INL MCM test bed functions as the cold water source (condenser), while the pump (PUMP 4) is the pump for this cold water supply subsystem. The functionality of this subsystem is to provide cold water to the subsequent system at a required pressure and flow rate. To obtain the desired functionality, the following valve settings are used which corresponds to nominal operation in our experiments:

1 BV1, BV2, BV3, BV8, BV9, BV10: open;
2 All remaining BV valves closed;
3 BFV and GV manipulated for control.

4.1.2. *Valve subsystem*

The valve subsystem consists of valves and connecting tubing. This part of the system is also realized through the MCM test bed. The butterfly valve (BFV) and the glove valve (GV) function are used to modify the cooling water flow rate to the reactor subsystem, which is computer simulated. Hence, in reality, the flow is sent back to the MCM test bed reservoir (TANK). Thus, in the physical HiL experiment setup, the heat exchanger and condenser are not actually installed but modeled and the water is sent to a reservoir tank, replacing the condenser. We mention that the BFV is operated by means of two digital channels, respectively, for opening and closing of the valve. The corresponding signals are set by means of the developed GUI program. The GV is provided with

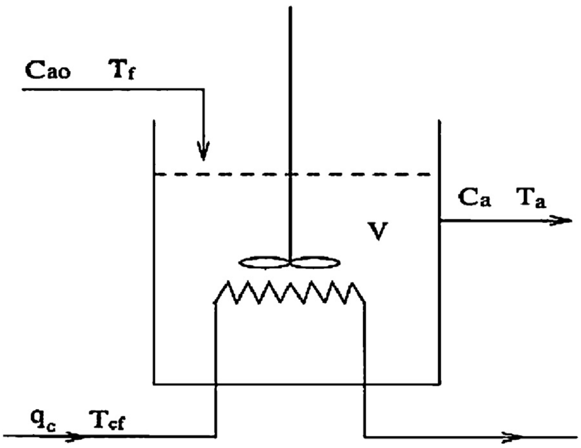


Fig. 7. The simulated CSTR reactor (taken from [37]).

a manufacturer-provided feedback controller which brings the valve position to a commanded setpoint. This setpoint is provided by means of the developed GUI program.

4.1.3. Reactor subsystem

For the reactor system, the model used by [36] is used. The major assumptions are that the reactor is a continuously stirred tank reactor (CSTR, perfect mixing) and converts a chemical species A to a chemical species B in a non-reversible manner. This reaction is exothermic and thus it is necessary to control the temperature to prevent unstable operation. This is done by means of running cooling water through a heat exchanging coil placed inside the reactor. Fig. 7 shows a scheme of the reactor.

The equations are as follows:

$$\dot{C}_a = \frac{q}{V}(C_{a0} - C_a) - a_0 C_a \exp\left(\frac{-E}{R\dot{T}_a}\right) \quad (4.1)$$

$$\dot{T}_a = \frac{q}{V}(T_f - T_a) + a_1 C_a \exp\left(\frac{-E}{R\dot{T}_a}\right) + a_3 q_c \left(1 - \exp\left(\frac{-a_2}{q_c}\right)\right)(T_{cf} - T_a), \quad (4.2)$$

where C_a and T_a are the concentration of species A and the temperature in the reactor tank, which are the two model states. The feed flow does not contain component B but contains component A, whose concentration is given by C_{a0}. The system is manipulated with the coolant flow rate, q_c, and the cooling water temperature, T_{cf}, both taken as measurements from the actual MCM test bed. See Section 5.2 for details. In [36], q (reactor feed flow rate), V (reactor volume) and, T_f (feed temperature) are given and fixed. This remains the same here for simulation in conjunction with the MCM test bed, except that an on/off control switch is considered to switch the feed flow on and off (via *A*4 in Fig. 5). This is used as a last resort to maintain safety. Without such a safety measure, the exothermic nature of the chemical reaction can lead to a run-away reaction which can further lead to dangerous temperature and pressure levels, in turn leading to reactor explosion. Note this on/off switch affects the reactor feed flow rate only and not the cooling flow rate. Finally, a_1, a_2 and a_3 are fixed parameters of the model that quantify the stoichiometry, heat production and heat transfer, respectively. These parameters can be computed as in [36,37]. For simulation purposes, the variables q, V, T_f and parameters a_1, a_2, and a_3 are set so that a cooling flow of 250 gpm will result in a change in cooling water temperature of about 20K (~36 F).

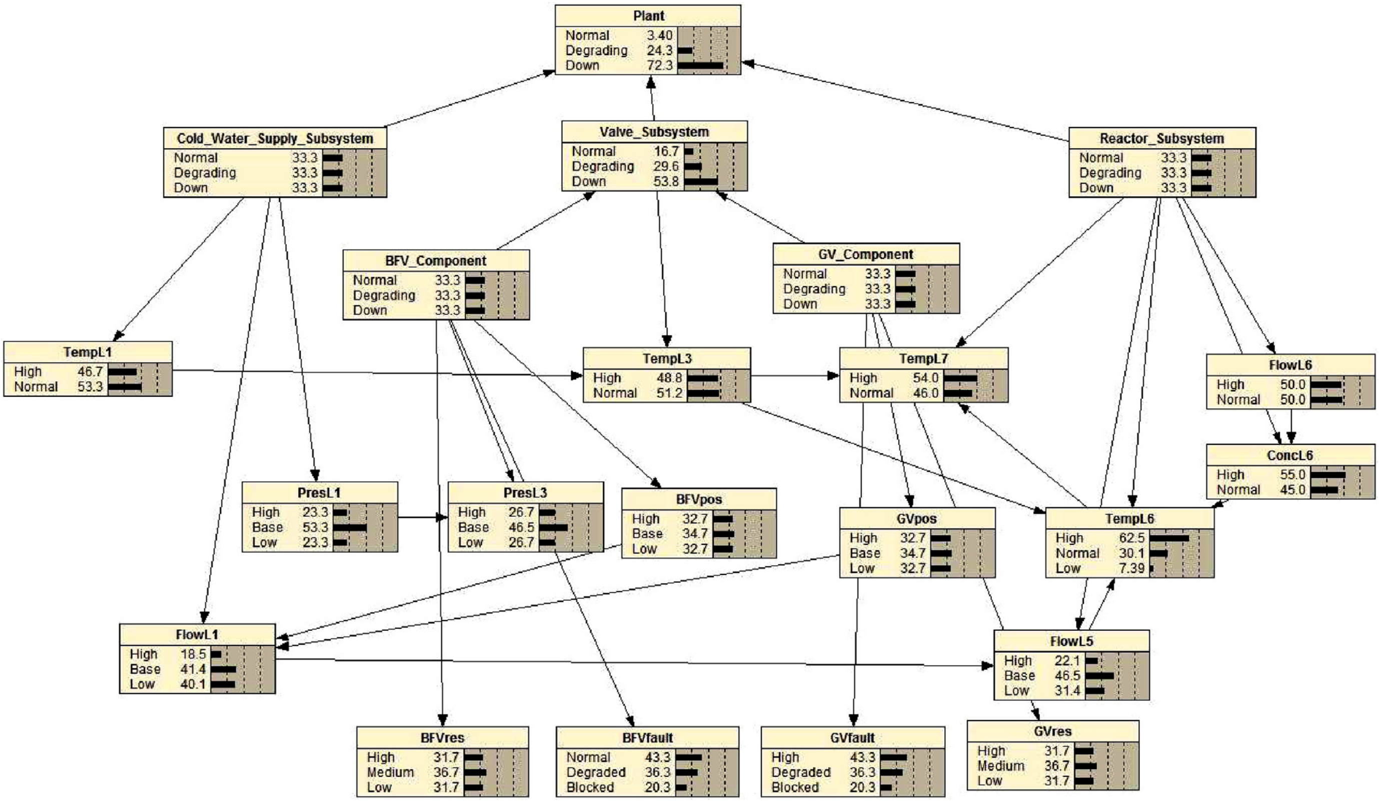


Fig. 8. BBN for the monitored plant considered.

Table 1
List of sensors with their attributes.

Index	Sensor label	Location	Real/virtual	Source signal	Variable type
1	TempL1_1	L1	Real	TT2	Temperature
2	TempL1_2	L1	Virtual	Sensing simulator	Temperature
3	FlowL1_1	L5	Virtual	Sensing simulator	Flow rate
4	FlowL1_2	L5	Virtual	Sensing simulator	Flow rate
5	PresL1_1	L1	Real	PT2	Pressure
6	PresL1_2	L1	Virtual	Sensing simulator	Pressure
7	BFVpos_1	L2	Real	ZT	Position
8	BFVpos_2	L2	Virtual	Sensing simulator	Position
9	PresL3_1	L3	Real	PT1	Pressure
10	PresL3_1	L3	Virtual	Sensing simulator	Pressure
11	TempL3_1	L3	Real	TT1	Temperature
12	TempL3_2	L3	Virtual	Sensing simulator	Temperature
13	GVpos_1	L4	Real	GV	Position
14	GVpos_2	L4	Virtual	Sensing simulator	Position
15	FlowL5_1	L5	Real	FT	Flow rate
16	FlowL5_2	L5	Virtual	Sensing simulator	Flow rate
17	FlowL6_1	L6	Virtual	Sensing simulator	Flow rate
18	FlowL6_2	L6	Virtual	Sensing simulator	Flow rate
19	ConcL6_1	L6	Virtual	Sensing simulator	Concentration
20	ConcL6_2	L6	Virtual	Sensing simulator	Concentration
21	TempL6_1	L6	Virtual	Sensing simulator	Temperature
22	TempL6_2	L6	Virtual	Sensing simulator	Temperature
23	TempL7_1	L7	Virtual	Sensing simulator	Temperature
24	TempL7_2	L7	Virtual	Sensing simulator	Temperature

4.1.4. Instrumentation

Table 1 indicates the sensors placed in the monitored system, together with their attributes, namely: location; whether they are actually present in the MCM test bed or whether they are virtual sensors; what their source signal is; and the type of process variable they measure. In the simulated system, each process variable considered is assumed to be measured twice. In the case an actual sensor is available, this means that a second, virtual sensor is placed in the same pod. In the other case, both sensors are virtual. All virtual sensors have emulation as their source, which is implemented in the sensing simulator module as explained in Section 5.2. In total, 12 × 2 =24 sensors are available.

Table 2 indicates the actuators placed in the monitored system together with their attributes, namely: location; whether they are actually present in the MCM test bed or whether they are virtual actuators; and the target channel of the actuator signal. The four control signals are labeled *A*1 to *A*4 as in Fig. 5 and correspond to the BFV controlling channels DO:open and DO:close; the GV setpoint signal (AO: glove valve); and the reactor feed flow, respectively.

4.2. BBN for monitored plant

Fig. 8 illustrates the BBN modeling the causal relations among the process variables in the monitored plant. This BBN is used in the ReCAM system plant assessment layer to assess the overall health of the plant.

The node “Plant” represents the overall health of the plant, which can be normal, degrading, or down. As described in Section 3.2.3, when the entropy of the probability distribution of this node decreases below a user specified decision threshold, a definite decision about the overall health of the plant is made and the BBN is reset. Likewise, the nodes “Cold_Water_Supply_Subsystem,” “Valve_Subsystem,” and “Reactor_Subsystem,” represent the health of the cold water supply, valve, and reactor subsystems, respectively, while the nodes “BFV_Component” and “GV_component” represent the health of the BFV and GV, respectively. The two nodes “BFVfault” and “GVfault” are added to accommodate for the health assessments from the Kalman filter-based methods described in Section 3.3. The other nodes, except for “BFVres” and “GVres,” represent the measured process variables, each measured by two sensors described in Table 1. The nodes “BFVres” and “GVres” represent two additional variables that are differences between the measured BFV and GV positions and their respective setpoints. These variables provide information on whether the valves are being controlled as desired. Probability distribution estimates of these two variables are calculated in the usual way as described in Section 3.2.2 using the valve position sensor DQs (i.e., the DQs of BFVpos_1, BFVpos_2, GVpos_1, GVpos_2). Note that the four root nodes of this BBN are “Cold_Water_Supply_Subsystem,” “BFV_Component,” “GV_component,” and “Reactor_Subsystem.” Hence, when resetting the BBN, each possible state of these nodes is accordingly assigned with equal probability.

Table 2
List of actuators with their attributes.

Index	Actuator label	Location	Real/virtual	Target
1	A1	L2	Real	Channel: DO:open
2	A2	L2	Real	Channel: DO:close
3	A3	L4	Real	Channel: GV
4	A4	L6	Virtual	Reactor simulator module

4.3. Supervisory control

The next sections describe the control strategies designed for the ReMAC system. The supervisory controller, which selects the best regulatory controller given plant health assessments, is first described, followed by the particular candidate regulatory control strategies.

4.3.1. Supervisory control

The supervisory controller is implemented as a state machine, in which the states represent the active control strategies (CTRL1–5) and state transitions represent the switches between them. The structure of such state machines can be represented in a general fashion by means a directed bipartite graph, where the nodes are the states (controllers) and the events (transitions). The states are tied to the corresponding controllers. The events are triggered based on inputs from the Kalman filter-based methods and the ReCAM system. Fig. 9 shows a supervisory controller, in which a move from one control configuration to the next does not allow a return to the previous control configuration.

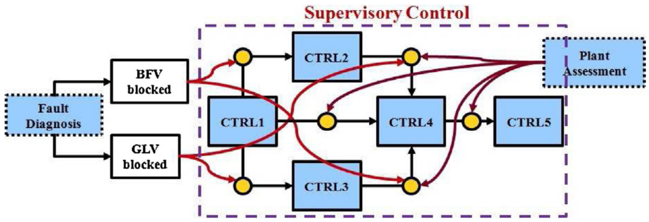
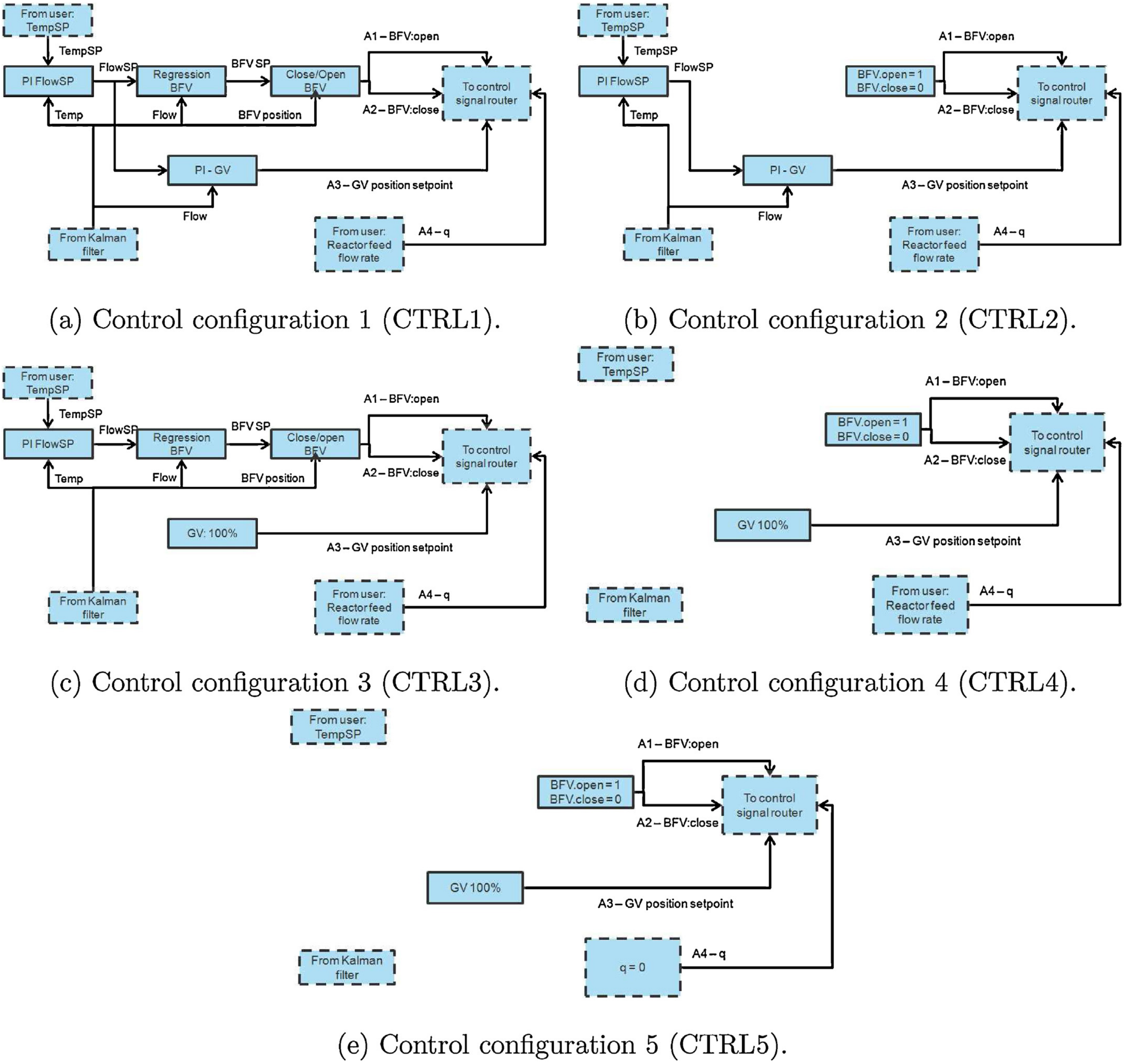


Fig. 9. State machine implementation of supervisory controller.

The underlying idea is that there are no tools considered available within the foreseen tests that would enable to fix the encountered problems (e.g. BFV blocking cannot be fixed). Hence, this supervisory controller structure is effective to showcase the benefits of using a ReMAC system with a control system that can only degrade. Although Fig. 9 shows the fully automated supervisory controller decision process, in the performed experiments, it remained possible for the human operator to reset the supervisory controller by returning its state to the CTRL1 state while simultaneously also resetting the Kalman filter and diagnosis modules. This allows repeated experimentation in case of erroneous diagnostic results, possibly due to the stochastic characteristics in the monitored process or sensor signals. The transitions between control configuration are controlled by two sources of information. The first source of information is the Kalman filter-based methods. In the case that this module indicates that the BFV and/or GV valve is blocking, the appropriate transition is made, depending on the current state. This affects transitions between configuration CTRL1–CTRL4. The second source of information is the plant assessment based on the ReCAM system. If the plant is considered to be in a bad condition as a whole for a given assessment (e.g., if the system



(a) Control configuration 1 (CTRL1).

(b) Control configuration 2 (CTRL2).

(c) Control configuration 3 (CTRL3).

(d) Control configuration 4 (CTRL4).

(e) Control configuration 5 (CTRL5).

Fig. 10. Candidate regulatory control strategies.

is down), then a transition is made. The first time this happens, this is from CTRL1, CTRL2 or CTRL3 to CTRL4. If the bad condition persists, then the state machine switches from CTRL4 to CTRL5, thus leading to shutdown of the plant. The underlying idea is that at this point it has become impossible to maintain safe plant operation (e.g., preventing reactor explosion) without shutting it down.

4.3.2. Regulatory controls

The following candidate regulatory control strategies, shown in Fig. 10, account for different possible conditions as assessed by the Kalman filter-based methods and the ReCAM system. The first strategy (Fig. 10(a)) is the default and assumes complete functionality of the monitored system. The second to fifth strategies (Fig. 10(b)–(e)) assumes that one or more components in the system are failing or faulty.

Reactor temperature control via BFV and GV (CTRL1; default): This control configuration is used in normal operations. It consists of the cascade control structure shown in Fig. 10(a). The objective of this controller is to maintain the reactor temperature at a safe setpoint in an efficient manner (i.e. limiting the amount of valve position changes). The outer loop sets the flow rate setpoint so to maintain the temperature in the reactor at the given setpoint using a proportional-integral (PI) controller, shown as block "PI FlowSP." The inner loop controls the valve positions to obtain the desired flow rate setpoint as given by the outer loop. Both valves are used to accomplish this. Subject to severe hysteresis, the BFV is set to a value which guarantees a 10% higher flow than the setpoint. This is based on a piecewise linear regression curve which upper bounds the already established hysteresis curve, shown as block "Regression BFV." There are two actual signals, $A1$ and $A2$, to be sent. While $A1$ gives BFV the open command, $A2$ gives the close command. These signals are sent to a control signal router, which routes them to the appropriate locations in Fig. 5. The BFV setpoint is compared to the available BFV position estimate from the Kalman filter and $A1$ and $A2$ are adjusted accordingly (Close/Open BFV). The BFV controller is responsible for tracking the flow rate setpoint to a large extent but not for disturbance rejection. The GV valve is used for regulating the cooling flow rate to setpoint precisely by means of a PI controller, shown as block "PI – GV." The resulting GV control signal, $A3$, is sent to the control signal router, which routes them to the appropriate locations in Fig. 5. This PI controller is used for tracking the setpoint as well as disturbance rejection. Finally, the reactor feed flow rate, which is not used for control, is fixed to its nominal rate and sent without modification to the control signal router in the simulated system.

Reactor temperature control via GV only (CTRL2): This control configuration is used when the BFV is not available for control because (1) the BFV sensor signal is not available and/or (2) the BFV valve is blocked. The objective of this controller is to maintain the reactor temperature at a safe setpoint by limiting the amount of valve position changes for the GV. The default control strategy (CTRL1) is modified as follows to obtain this strategy, shown in Fig. 10(b). The BFV regression-based control element is removed and replaced by ordering BFV to open to maximal range. In the case that the BFV unavailability is due to a sensor malfunction, maximal rangeability for GV is obtained since the BFV will not limit the flow. In the case the BFV valve is blocked, this has no effect. However, since it is not necessarily known which one is the case, opening the BFV is the best available control action. All other elements are structurally the same. Parametrically, a more aggressive tuning is used for PI – GV element because this PI controller is now responsible for both flow rate setpoint tracking and disturbance rejection.

Reactor temperature control via BFV only (CTRL3): This control configuration is used when the GV is not available for control because (1) the GV sensor signal is not available and/or (2) the GV is blocked. The objective of this controller is to maintain the reactor temperature at a safe setpoint or a lower setpoint by setting the BFV position. The default control strategy (CTRL1) is modified as follows to obtain this strategy, shown in Fig. 10(c). The GV PI control element is removed and replaced by ordering the GV to open to maximal range (100%). In the case that the GV unavailability is due to a sensor malfunction, maximal rangeability for the BFV valve is obtained in this case since the GV will not limit the flow. In the case the GV is blocked, this has no effect. However, since it is not necessarily known which one is the case, opening the GV is the best available control action. All other elements are structurally and parametrically the same. Hence, the flow rate will generally be higher than desired because the BFV regression element is conservative in the sense that it provides a higher flow than the setpoint by design.

Maximize heat transfer (CTRL4): This control configuration is used when (1) neither BFV or GV are available for control or (2) the reactor temperature is dangerously high so that maximum heat transfer is required. The objective of this controller is to maintain the reactor temperature at a minimal level in the scenarios that (1) both valves are unavailable or (2) configurations CTRL1 to CTRL3 do not lead to effective satisfaction of the setpoint requirements for the reactor temperature. The first scenario results when:

- the BFV sensor signal is not available and/or the BFV is blocked; *and*
- the GV sensor signal is not available and/or the GV is blocked.

The second scenario results from an increase in the feed flow rate or from a reduced heat exchange capacity. The latter, in turn, may be due to pipe congestion. The default control strategy (CTRL1) is modified as follows to obtain this strategy, shown in Fig. 10(d). The BFV regression-based control element is removed and replaced by ordering the BFV to open to maximal range. Similarly, the "GV PI" control element is removed and replaced by ordering the GV to open to maximal range (100%). All other elements are removed.

Shut-down operation (CTRL5): This control configuration is the configuration used as a last resort to maintain safety. The objective is to prevent explosion of the reactor. It is used when the CTRL4 configuration is used and still leads to insufficient heat transfer capacity. It is a simple modification of CTRL4 in the sense that the reactor feed flow rate is forced to be zero. Fig. 10(e) shows the corresponding scheme.

5. Implementation

In this section, we describe software implementation of the developed ReMAC system and simulations of the monitored plant considered.

5.1. Software implementation of ReMAC system

An overview of the software implementation of the developed ReMAC system in connection to the monitored plant considered is shown in Fig. 11. In particular, the ReCAM system architecture, shown in Fig. 1, is implemented in Matlab and the Bayesian belief network used by the ReCAM system for plant assessments shown in Fig. 8 is implemented in the software Netica, where JAVA API is used to establish connection between Netica and Matlab.

As the cold water supply and valve subsystems of the monitored plant are implemented by the MCM testbed, a data acquisition interface is used to communicate data to and from the MCM testbed. The reactor subsystem of the monitored plant is implemented in LabVIEW using signal data from the MCM testbed for Eq. (4.1). Moreover, a graphical user interface (GUI) is also implemented in LabVIEW. Fig. 12 shows a snapshot of part of this GUI.

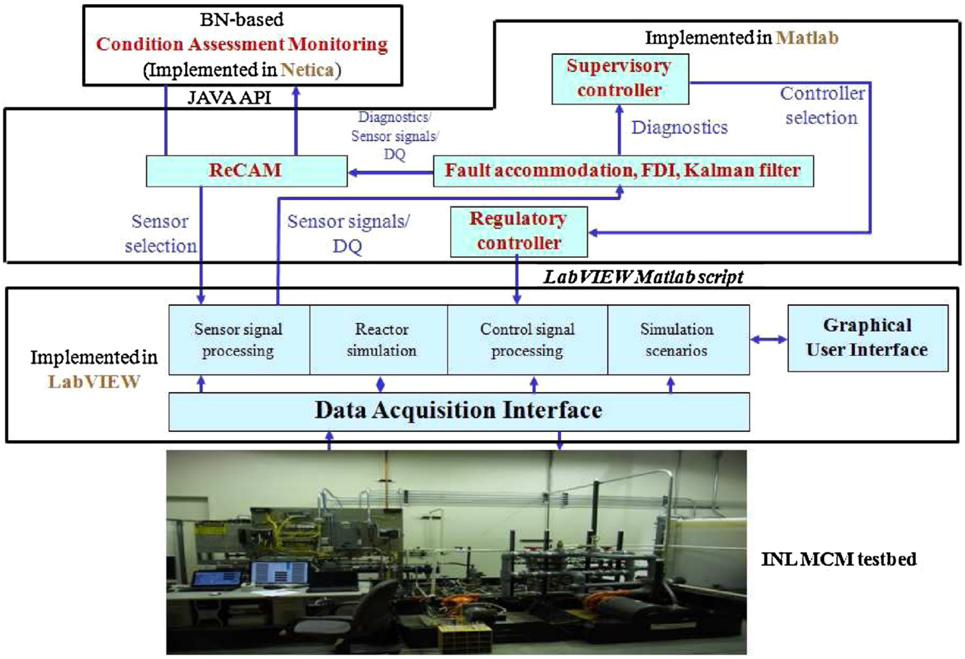


Fig. 11. Software implementation of ReMAC system in connection to the monitored plant.

This GUI interface allows operators to set simulation scenarios such as physical anomalies and cyber attacks considered and displays results such as current component and systems-centric monitoring results, the state of the supervisory controller (i.e., the current regulatory control used), and various process variable values. In addition, implementations in LabVIEW include routines that route control signals to appropriate actuator locations and that filter sensor signals in accordance to ReCAM system sensor selections. Communications between implementations in LabVIEW and Matlab is achieved through the LabVIEW Matlab script.

5.2. Monitored plant simulation

This section describes how the monitored plant is simulated in an HiL experimental implementation as illustrated in Fig. 13.

In the following description, the normal (no faults) information flow is described, while in Section 6.1, the faults and their realizations are explained. At the right side of Fig. 13, all the control signals from regulatory control are routed to the data logging. The same control signals are split into the signals A1 to A3, which are sent to the data acquisition (DAQ) system to further send them to the actual MCM test bed. In contrast, A4 (reactor feed) is sent to the reactor simulator. All the sensor signals are sent to a sensing simulator, which is used to create the virtual sensor signals in addition to the real sensor signals. The sensor signals FT (flow rate) and TT2 (temperature) are sent directly to the reactor simulator from the DAQ system and mapped to the variables q_c (cooling flow rate) and T_{cf} (cooling flow temp.) for simulation. While sensor signals FT and TT2 are subject to measurement noise and thus do not reflect the true states in the MCM test bed, they are used without modification for simulation purposes, thus simulating process disturbances in the reactor and adding more realism to the reactor simulation. The reactor simulator provides the true (no measurement noise added) values for q, C_a, T_a (i.e., the feed flow rate, concentration of species A, and reactor temperature, respectively) following Eq. (4.1). These are sent to a data logger module as well as to the sensing simulator.

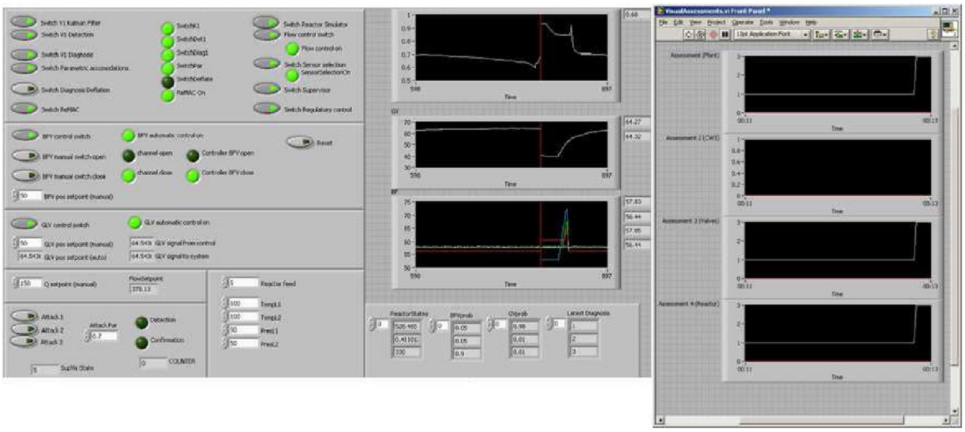


Fig. 12. GUI developed for ReMAC.

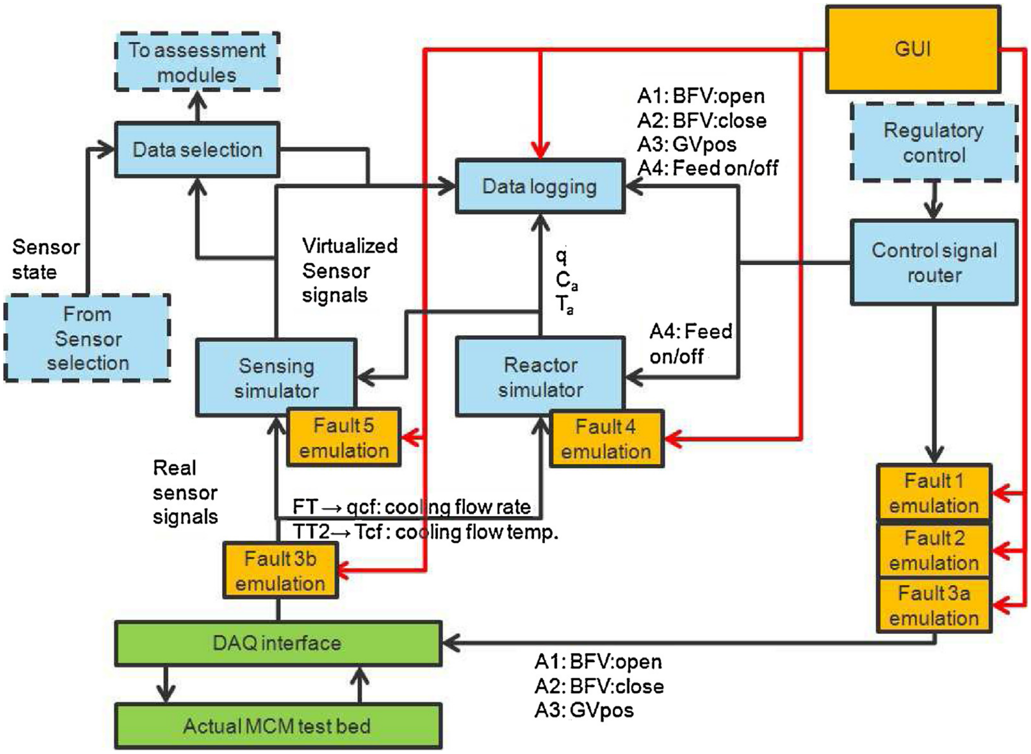


Fig. 13. Simulation of the monitored plant with the physical MCM testbed.

The sensing simulator is used to create the additional sensor signals necessary for the virtual sensors listed in Table 1. The resulting signals are sent to a data logger and to the sensor selector (see below). Within the sensing simulator, the following three different cases are recognized:

Case 1: a real sensor exists (signals from DAQ system). In this case, the original real signal is kept as is and the second signal is created by adding additional noise amounting to 5% of the noise variance in the original signal.
Case 2: signals from reactor simulator. In this case, independent noise with a standard deviation of 1% of the nominal value is added to the true, simulated signal to obtain two virtual sensors.
Case 3: a copy signal from another sensor. In this case, an additional sensor based on a measurement on another location is emulated by copying the original signal and adding 5% of the noise variance in the copied signal. Specifically, this is done to obtain the FlowL1_1 and FlowL1_2 measurements (copy of real signal FlowL5_1) and for TempL7_1 and TempL7_2 measurements (copy of TempL6_1 and TempL6_2).

The signals generated above are sent to the data logger and to data selection. This last module practically implements the sensor selection strategy by replacing the sensor signal in those sensors not selected by a code value specifying a not measured quantity.

6. Results

6.1. Fault and failure scenarios

6.1.1. Physical anomalies/attacks

The following physical anomalies/attacks (faults and failures) are considered for evaluation of the developed ReMAC system.

Physical Anomaly/Attack #1: BFV blocked (failure): This is artificially introduced by suppressing the digital control signals, no matter what the regulatory control modules provides as a signal. This fault is introduced by a module between the control signal router block and the DAQ system (Fig. 13). In mathematical terms:

$$\begin{cases} A1_{faulty}(t) = A1_{normal}(t) & t < t_f \\ A1_{faulty}(t) = 0 & t \geq t_f, \\ A2_{faulty}(t) = A2_{normal}(t) & t < t_f, \\ A2_{faulty}(t) = 0 & t \geq t_f, \end{cases} \tag{6.1}$$

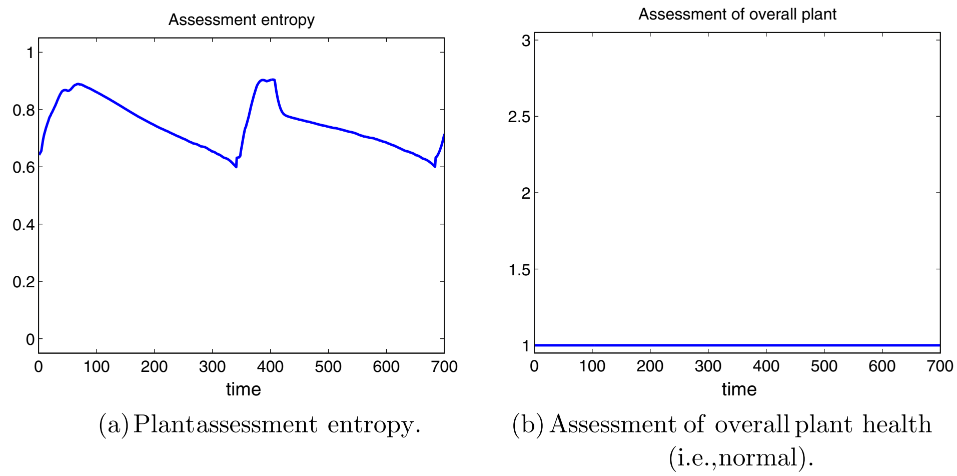
where t_f is the start time of the fault. Initially, this fault may not result in any symptoms as the system may be functioning in steady state. If the setpoint for the reactor temperature is higher than the current temperature, then the controller will command the valve to open. Since this cannot happen, the valve position, pressure drop over the BFV, and flow rate will not increase as expected. Furthermore, the reactor temperature and exit cooling water temperature may further increase to dangerous levels.

Physical Anomaly/Attack #2: GV blocked (failure): This is artificially introduced by keeping the GV setpoint constant, no matter what the regulatory control modules provides as a signal. This fault is introduced by a module between the control signal router block and the DAQ system (Fig. 13). In mathematical terms:

$$\begin{cases} A3_{faulty}(t) = A3_{normal}(t) & t < t_f, \\ A3_{faulty}(t) = A3_{normal}(t) & t \geq t_f, \end{cases} \tag{6.2}$$

where t_f is the start time of the fault. Initially, this fault may not result in any symptoms as the system may be functioning in steady state. If the setpoint for the reactor temperature is higher than the current temperature, then the controller will command the valve to open. Since this cannot happen, the valve position, pressure drop over the BFV, and flow rate will not increase as expected. Furthermore, the reactor temperature and exit cooling water temperature may further increase to dangerous levels.

Physical Anomaly/Attack #3: Pipe congestion (fault): A partial congestion of the pipes is artificially introduced by linearly reducing



(a) Plantassessment entropy.

(b) Assessment of overall plant health (i.e.,normal).

Fig. 14. Plant assessment entropy and assessment of overall plant health for Scenario 1.

the GV range down to a fraction R (e.g., 20%) of its range in a timer period Δt by modifying the GV setpoint as follows.

$$\begin{cases} A3_{faulty}(t) = A3_{normal}(t) & t < t_f \\ A3_{faulty}(t) = A3_{normal}(t)\left(1-(1-R)\min\left(\left(\frac{t-t_f}{\Delta t}\right),1\right)\right) & t \geq t_f \end{cases} \tag{6.3}$$

with t_f the start time of the fault. The parameters R and Δt are introduced via the GUI. This part of the fault is introduced by a module between the control signal router block and the DAQ system. Simultaneously, the GV position measurements are magnified (up to 400%) as follows:

$$\begin{cases} GV_{fault} = GV_{true} & t < t_f \\ GV_{fault} = GV_{true}/\left(1-(1-R)\min\left(\left(\frac{t-t_f}{\Delta t}\right),1\right)\right) & t \geq t_f \end{cases} \tag{6.4}$$

This part of the fault is introduced by a module between the control signal router block and the DAQ system. By simultaneous modification of both the GV setpoint and measurement, the cool water flow appears to be smaller than that in normal settings (i.e., without the simultaneous modifications) for a measured GV position. As a result, this artificially introduces a partial congestion of the pipes. For realism, care needs to be taken that the absolute rate (percentage/second) by which the setpoint changes is smaller than the speed of GV motor.

Physical Anomaly/Attack #4: Extreme feed flow (fault): A problem in the reactor system is simulated as follows. The feed flow rate is increased up to a multiple, M (e.g., 200%), of its normal level, leading to extra heat production, which is hard to cool down. To this end, the feed flow rate used for reactor is modified as follows:

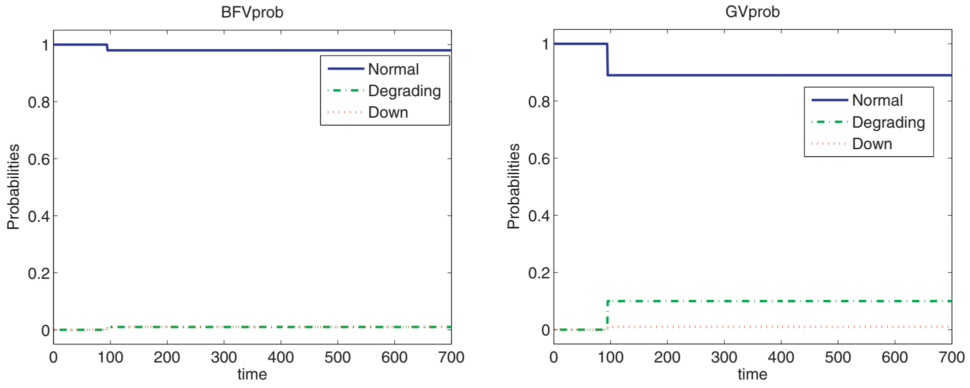
$$q_{fault} = qM, \tag{6.5}$$

where q is fixed and internal to the model, and M is the multiple provided via the GUI.

6.1.2. Cyber attacks

Cyber attacks that compromise sensor measurements are considered. In particular, measurements of attacked sensors are modified so that they provide readings, which make the system condition seem worse than it actually is. As high temperatures, pressures, and flow rates are typically to be avoided, considered cyber attacks add positive bias to sensor readings. Moreover, cyber attacks are also considered that modify position measurement of BFV and GV so that they are viewed to be saturated (e.g., a bias positive value which makes the signal close to or over the maximum opening value).

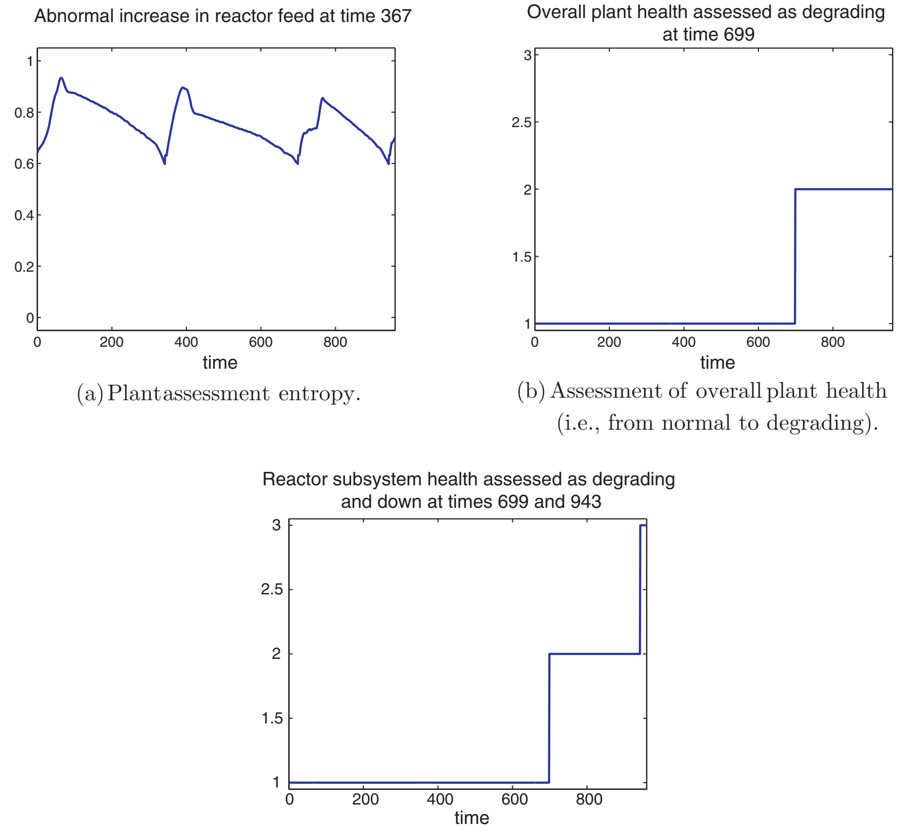
DQs quantifying trustworthiness of sensor data are assigned by a watched dog system mentioned in Section 2. The value of DQ is a number in [0, 1], where 0 indicates the sensors data is worthless and



(a) Health of butterfly valve (BFV).

(b) Health of glove valve (GV).

Fig. 15. Health of butterfly and glove valves in terms of probabilities under Scenario 1.



(a) Plantassessment entropy.

(b) Assessment of overall plant health (i.e., from normal to degrading).

(c) Assessment of reactor subsystem health (i.e., from normal to degrading to down).

Fig. 16. Plant assessment entropy, assessment of overall plant health, and reactor subsystem health under Scenario 2.

1 indicates that the sensor data is trustworthy. In our experiments, DQs of data from sensors that are attacked are assigned to 0.1, while data from those that are not attacked are assigned to 0.95.

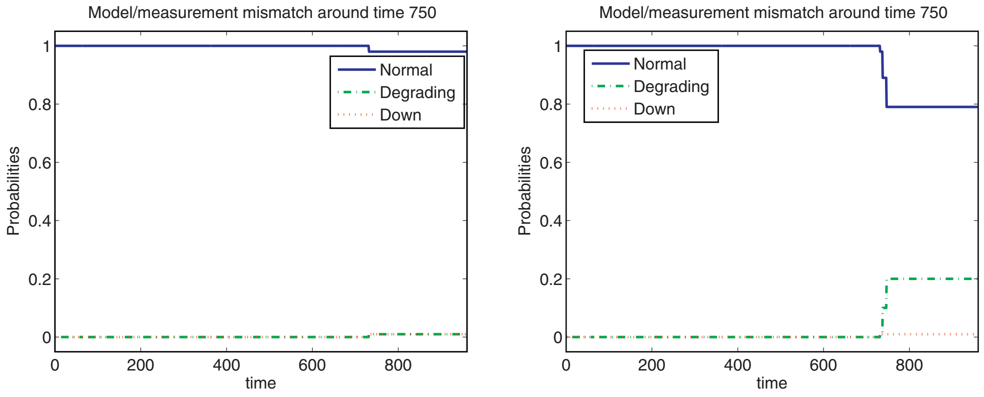
6.2. Scenarios

Three scenarios are considered for experimental HiL verification of the developed ReMAC system:

Scenario 1: The experimental trail is conducted for 700 s, during which neither physical anomalies nor cyber attacks occur. The purpose of this scenario is to verify that the developed ReMAC system makes correct assessments when the monitored system is normal.

Scenario 2: The experimental trail is conducted for 900 s, where an abnormal increase in reactor feed (i.e., Physical Anomaly/Attack #4 in Section 6.1.1) occurs at time 367 (M changes from 0.25 to 4 in (6.5)). However, there are no cyber attacks. The purpose of this scenario is to verify that the developed ReMAC system makes correct assessments when a physical anomaly occurs in the monitored system.

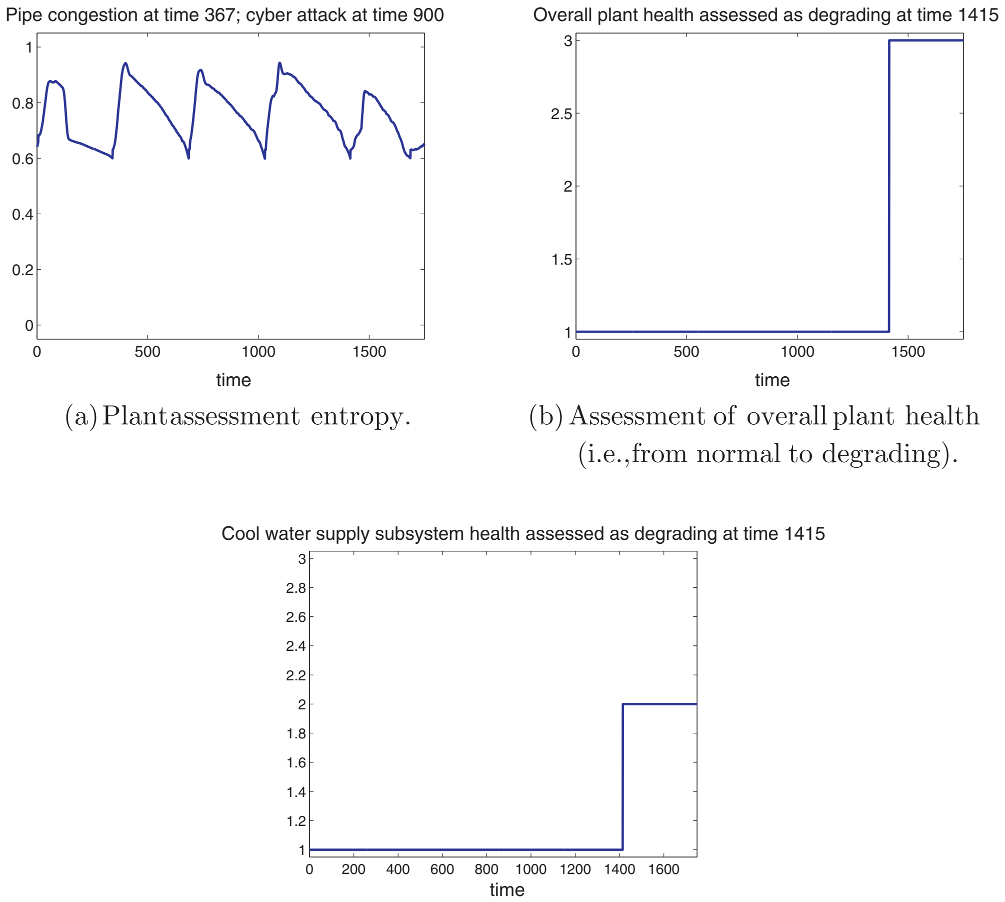
Scenario 3: The experimental trail is conducted for 1700 s, where pipe congestion (i.e., Physical Anomaly/Attack #3 in



(a) Health of butterfly valve (BFV).

(b) Health of glove valve (GV).

Fig. 17. Health of butterfly and glove valves in terms of probabilities under Scenario 2.



(a) Plantassessment entropy.

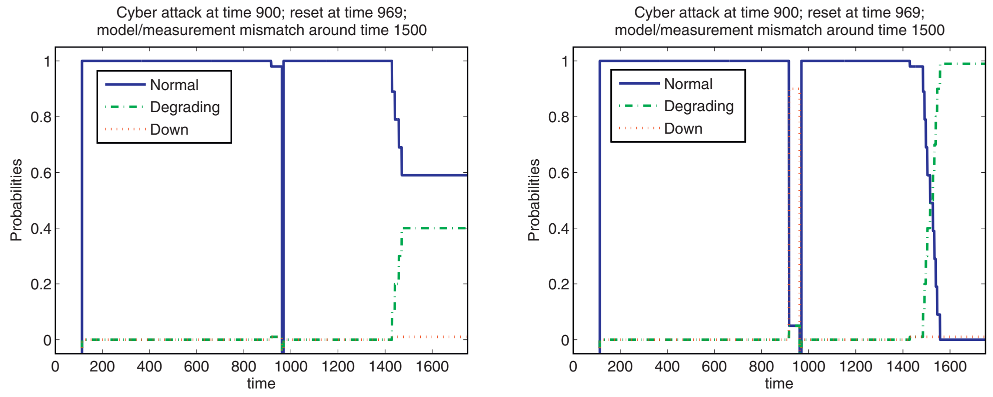
(b) Assessment of overall plant health (i.e.,from normal to degrading).

(c) Assessment of cold water supply subsystem health (i.e., from normal to down).

Fig. 18. Plant assessment entropy, assessments of overall plant health, and cold water supply subsystem health under Scenario 3.

Section 6.1.1) starts to occur with $R = 60\%$ and $\Delta t = 300$ in (6.3) and (6.4) at time 85. Moreover, cyber attacks on sensors are conducted at around time 900. In particular, sensor GVpos_1 incorrectly shows that GV is stuck, while sensors Temp1_1, Temp1_2, Pres1_1, and Pres1_2 incorrectly show high temperatures and pressures. The purpose of this scenario is to verify that the developed ReMAC system makes correct assessments when a physical anomaly occurs in the monitored system and sensors are attacked.

Moreover, we mention that the (user-defined) desired decision period described in Section 3.2.4 is 350, 250, and 150 s when (definite) physical health assessments of the system (described in Section 3.2.3) is normal, degrading, or down, respectively.



(a) Health of butterfly valve (BFV).

(b) Health of glove valve (GV).

Fig. 19. Health of butterfly and glove valves in terms of probabilities under Scenario 3.

Moreover, definite decisions of the monitored system health is made when assessment entropy decreases below the threshold 0.6.

6.3. *Experiment results*

This section describes results for the three scenarios described above.

Scenario 1: Fig. 14(a) shows the plant assessment entropy from the ReCAM system described in Section 3.2.3. In particular, ReCAM makes a definite assessment of the overall plant when the plant or physical health assessment entropy decreases below the threshold 0.6 and subsequently resets the BBN. Whenever the ReCAM system makes a (definite) assessment of the overall monitored plant, this assessment is kept until the next (definite) assessment. The saw-tooth behavior of the plant assessment entropy arises from the fact that, after the BBN is reset and as sensor observations are gathered, the ReCAM system first reverses its initial belief of the plant (entropy increase) and then converges toward an assessment consistent with the sensor observations (entropy decrease). With normal, degrading, and down assessments corresponding to the numbers 1, 2, and 3, respectively, Fig. 14(b) illustrates the (definite) assessment of the overall monitored plant by the ReCAM system with the assumption that the system is normal at start. We note that the monitored system health is correctly being assessed as normal (i.e., 1) throughout the experiment. By inspecting Fig. 14(a), we also note that the decision periods (i.e., time periods between definite assessments of the system or resettings of the BBN) are roughly 350 s as desired. Fig. 15(a) and (b) illustrates the probability distributions of the BFV and GV health calculated by Kalman filter-based diagnostic methods. As these valves are not blocked, the probabilities of these two valves being healthy are quite high throughout this experimental trail.

Scenario 2: Fig. 16(a) shows the plant assessment entropy from the ReCAM system, while Fig. 16(b) illustrates the (definite) assessment of the overall monitored plant by the ReCAM system with the assumption that the system is normal at start. The reason of the saw-tooth behavior in Fig. 16(a) is the same as one for Fig. 14(a). We note that the monitored system health is correctly being assessed as degrading (i.e., 2) at time 699, which is the first definite decision made after Physical Anomaly/Attack #4 occurred. By inspecting Fig. 16(a), we also note that, as desired, the decision periods are roughly 350 and 250 s, respectively, before and after the system is determined to be degrading. As a further illustration, Fig. 16(c) shows the assessments of the reactor subsystem, which is correctly determined to be degrading at time 699. Moreover, as the supervisory control is turned off for this particular experimental trial, no actions are taken to address the reported health assessments. Hence, the situation worsens and the reactor subsystem is assessed to be down at the next (definite) decision (time 943). Fig. 17(a) and (b) illustrates the probability distributions of the butterfly and glove valve health calculated by Kalman filter-based diagnostic methods. As these valves are not blocked, the probabilities of these two valves being healthy are quite high throughout the experimental trail. However, at around time 750, these probabilities decreased a little bit due to a slight mismatch between the assumed model and measurement. This phenomenon is also observed in Scenario 3 (Fig. 19) and described in detail there.

Scenario 3: Fig. 18(a) shows the plant assessment entropy from the ReCAM system, while Fig. 18(b) illustrates the (definite) assessment of the overall monitored plant by the ReCAM system with the assumption that the system is normal at start. As the parameters chosen here for Physical Anomaly/Attack #3 indicates that the pipe congests slowly, the monitored system health is correctly being assessed as degrading (i.e., 2) at time 1415, which is the 4th definite decision made after the pipe starts to congest. We also note that, as desired, the decision periods are roughly 350 and 250 s, respectively, before and after the system is determined to be degrading. Furthermore, as pipe congestion causes decreased cool water flow, Fig. 18(c) shows that the cold water supply subsystem is determined to be degrading at time 1415. Fig. 19(a) and (b) illustrates the probability distributions of the butterfly and glove valve health calculated by Kalman filter-based diagnostic methods. Note that, after cyber attacks on the sensors are introduced around time 900, the probability that the GV is down becomes (incorrectly) high. The reason for this observation is that Kalman filter-based assessments do not utilize sensor DQs and are prone to mistakes when cyber attacks are conducted. However, as inspection indicates that the GV is normal, we reset the Kalman filter-based assessment algorithm around time 969, causing the probability of the glove valve normal to be high. Cyber attacks on the sensors do not effect on the definite decisions made by the ReCAM system regarding the overall plant health as sensor DQs are taken into account here. We note that in Fig. 19, the probabilities to be in a degraded condition for BFV and GV both became high around time 1500. In both cases, mismatch between model and measurement is considered the root cause of the diagnoses. In the case of BFV, a short-time opening signal, expected to open the valve, did not result in such opening due to valve backlash. While the model used in the Kalman filter includes backlash as a phenomenon, the associated backlash parameter is not always accurate. In the case of the GV, the actual measurement of the valve position hovered around 100.2% as a relative measure of opening, which is higher than the saturation level (100%) assumed in the model. Fig. 20 shows that the supervisory control correctly switches to CTRL4 (i.e., maximize heat transfer by opening BFV and GV to their maximum) after the system is determined to be degrading. The temporary switch to CTRL3 at time 917 is due to the incorrect assessment that the glove valve is blocked from the Kalman filter-based algorithm. The supervisor is switched back to CTRL1 when the Kalman filter-based algorithm is reset.

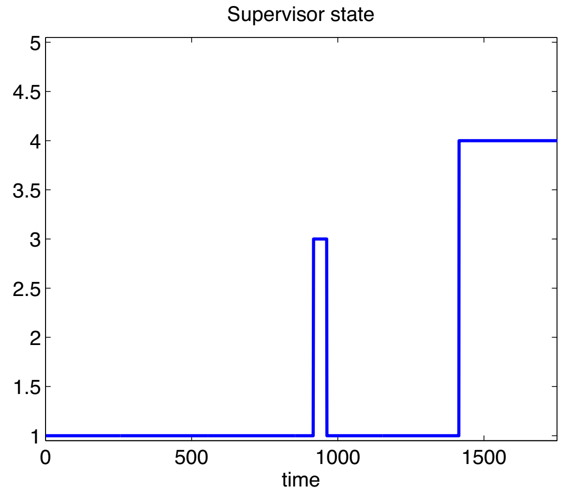


Fig. 20. State of supervisory controller.

7. Conclusion and future work

This paper experimentally demonstrated in an HiL configuration a ReMAC system that integrates previously developed systems- and component-centric monitoring algorithms with a supervisory controller, which selects, from a set of candidates, the best controller based on the current plant health assessments. The implemented ReMAC system is demonstrated on a chemical reactor with a water cooling system, where the reactor is computer simulated and the water cooling system is implemented by a MCM testbed at INL.

Results showed that the ReMAC system is able to make correct plant and component health assessments despite sensor malfunctioning/attacks and make decisions that achieve best control actions despite possible actuator malfunctioning/attacks. However, it is observed that erroneous diagnosis results may be reported by component-centric (Kalman filter-based) monitoring algorithms due to mismatch between assumed system component models and actual measurements. In addition to the above noted issue on Kalman filter-based algorithms, we mention other challenges to be fully analyzed and addressed in the future that are critical to the success of deploying a ReMAC system:

1. A ReMAC system requires redundancy in sensors. However, we note that this is common in, e.g., nuclear power plants.
2. The sensor signals need to provide“sufficient symptoms” for all considered process faults failures.
3. Component-centric fault diagnosis is restricted in the sense that only one fault can appear in one device at a single time.
4. Identifying the relationships among process variables and system conditions for constructing the BBN can be challenging. Moreover, once the structure of the BBN is determined, identifying the correct conditional probabilities characterizing relations among nodes in the BBN may also be challenging.
5. Since the BBN cannot contain cycles, it cannot include feedback loops which are commonplace in engineered systems. As such, the BBN approach might fail if these feedback loops lead to strongly coupled variables and the resulting relationship is not captured well by the BBN.

Besides the above challenges, future work also includes extending the developed ReMAC system to applications in power grid monitoring and protection.

Acknowledgments

The research reported here was supported by the Instrumentation, Control, and Intelligent Systems (ICIS) initiative at Idaho National Laboratory under U.S. Department of Energy contract DE-AC07-05ID14517. The authors would also like to thank Mr. Reed B. Carlson of the Idaho National Laboratory for his assistance in running the HiL experiments.

References

[1] H.E. Garcia, W.-C. Lin, S.M. Meerkov, A resilient condition assessment monitoring system, in: Proceedings of the 5th International Symposium on Resilient Control Systems, Salt Lake City, UT, 2012, pp. 98–105.

[2] K. Villez, B. Srinivasan, R. Rengaswamy, S. Narasimhan, V. Venkatasubramanian, Kalman-based strategies for fault detection and identification (FDI): Extensions and critical evaluation for a buffer tank system, Comput. Chem. Eng. 35 (5) (2011) 806–816.

[3] E. Hollnagel, D.D. Woods, N. Leveson, Resilience Engineering: Concepts and Percepts, Ashgate Publishing, Hampshire, England, 2006.

[4] H.E. Garcia, N. Jhamaria, H. Kuang, W.-C. Lin, S.M. Meerkov, Resilient monitoring system: Design and performance analysis, in: Proceedings of the 4th International Symposium on Resilient Control Systems, Boise, ID, 2011, pp. 61–68.

[5] E. Hollnagel, J. Pariès, D.D. Woods, J. Wreathall, Resilience Engineering in Practice: A Guidebook, Ashgate Publishing, Surrey, England, 2011.

[6] M.A. Moritz, M.E. Morais, L.A. Summerell, J.M. Carlson, J. Doyle, Wildfires, complexity, and highly optimized tolerance, Proc. Natl. Acad. Sci. 102 (50) (2005), pp. 17 912-17 917.

[7] Q. Zhu, T. Başar, Robust and resilient control design for cyber-physical systems with an application to power systems, in: Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference, Orlando, FL, December, 2011, pp. 4066–4071.

[8] C.G. Rieger, D.I. Gertman, H.A. McQueen, Resilient control systems: Next generation design research, in: Proceedings of the 2nd IEEE Conference on Human System Interaction, Catania, Italy, May, 2009, pp. 632–636.

[9] K. Ji, D. Wei, Resilient control for wireless networked control systems, Int. J. Cont. Autom. Syst. 9 (2) (2011) 285–293.

[10] K. Ji, Y. Lu, L. Liao, Z. Song, D. Wei, Prognostics enabled resilient control for model-based building automation systems, in: Proceedings of the 12th Conference of International Building Performance Simulation Association, 2011, pp. 286–293.

[11] R.S. Anderson, Cyber security and resilient systems, in: Proceedings of the 50th Annual Meeting of Institute of Nuclear Materials Management, 2009.

[12] M. Bishop, M. Carvalho, R. Ford, L.M. Mayron, Resilience is more than availability, in: Proceedings of the 2011 Workshop on New Security Paradigms, 2011.

[13] G.D.M. Serugendo, J. Fitzgerald, A. Romanovsky, N. Guelfi, A meta-based architectural model for dynamically resilient systems, in: Proceedings of the 2007 ACM Symposium on Applied Computing, 2007.

[14] K. Villez, V. Venkatasubramanian, H. Garcia, C. Reiger, T. Spinner, R. Rengaswamy, Achieving resilience in critical infrastructures: A case study for a nuclear power plant cooling loop, in: Proceedings of the 3rd International Symposium on Resilient Control Systems, Idaho Falls, ID, August, 2010, pp. 49–52.

[15] H.E. Garcia, W.-C. Lin, S.M. Meerkov, M.T. Ravichandran, Data quality assessment: Modeling and application in resilient monitoring systems, in: Proceedings of the 5th International Symposium on Resilient Control Systems, Salt Lake City, UT, 2012, pp. 124–129.

[16] H.E. Garcia, W.-C. Lin, S.M. Meerkov, M.T. Ravichandran, Resilient plant monitoring system: design, analysis, and performance evaluation, in: Proceedings of the 52nd IEEE Conference on Decision and Control, Florence, Italy, 2013, pp. 4983–4990.

[17] H.E. Garcia, W.-C. Lin, S.M. Meerkov, M.T. Ravichandran, Resilient monitoring systems: architecture, design, and application to boiler/turbine plant, IEEE Trans. Cybern. (2014).

[18] H.E. Garcia, W.-C. Lin, S.M. Meerkov, M.T. Ravichandran, Resilient monitoring system for boiler/turbine plant, in: Proceedings of the 6th International Symposium on Resilient Control Systems, San Francisco, CA, 2013, pp. 104–110.

[19] W.-C. Lin, H.E. Garcia, Inclusion of game-theoretic formulations for resilient condition assessment monitoring, in: Proceedings of the 6th International Symposium on Resilient Control Systems, San Francisco, CA, 2013, pp. 96–103.

[20] V. Venkatasubramanian, R. Rengaswamy, S.N. Kavuri, K. Yin, A review of process fault detection and diagnosis. Part iii: Process history based methods, Comput. Chem. Eng. 27 (3) (2003) 327–346.

[21] V. Venkatasubramanian, R. Rengaswamy, S.N. Kavuri, A review of process fault detection and diagnosis. Part ii: Qualitative models and search strategies, Comput. Chem. Eng. 27 (3) (2003) 313–326.

[22] K. Villez, V. Venkatasubramanian, R. Rengaswamy, Generalized shape constrained spline fitting for qualitative analysis of trends, Comput. Chem. Eng. 58 (11) (2013) 116–134.

[23] R.G. Brown, P.Y.C. Hwang, Introduction to Random Signals and Applied Kalman Filtering, John Wiley & Sons, Inc., New York, 1992.

[24] E. Wan, R. van der Merwe, The unscented Kalman filter, in: S. Haykin (Ed.), Kalman Filtering and Neural Networks, John Wiley & Sons, New York, 2001.

[25] I. Jolliffe, Principal Component Analysis, John Wiley & Sons, Ltd., New York, 2005.

[26] S. Roweis, EM algorithms for PCA and SPCA, Adv. Neural Inform. Process. Syst. 10 (1998) 626–632.

[27] M.E. Tipping, C.M. Bishop, Probabilistic principal component analysis, J. R. Stat. Soc. Ser. B (Stat. Methodol.) 61 (3) (1999) 611–622.

[28] P.R. Nelson, P.A. Taylor, J.F. MacGregor, Missing data methods in PCA and PLS: score calculations with incomplete observations, Chemometr. Intell. Lab. Syst. 35 (1) (1996) 45–65.

[29] S. Dash, M.R. Maurya, V. Venkatasubramanian, R. Rengaswamy, A novel interval-halving framework for automated identification of process trends, AIChE J. 50 (1) (2004) 149–162.

[30] T. Denceux, The cautious rule of combination for belief functions and some extensions, in: Proceedings of the 9th International Conference on Information Fusion, Florence, Italy, 2006, pp. 1–8.

[31] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, 1976.

[32] C.E. Shannon, A mathematical theory of communication, Bell Sys. Tech. J. 27 (3) (1948) 379–423.

[33] Y.-L. Huang, A.A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, S. Sastry, Understanding the physical and economic consequences of attacks on control systems, Int. J. Crit. Infrastruct. Protect. 2 (3) (2009) 73–83.

[34] Y. Peng, S. Zhang, R. Pan, Bayesian network reasoning with uncertain evidences, Int. J. Uncertain. Fuzz. Knowl.-Based Syst. 18 (5) (2010) 539–564.

[35] S.M. Meerkov, Mathematical theory of behavior-individual and collective behavior of retardable elements, Math. Biosci. 43 (1-2) (1979) 41–106.

[36] G. Lightbody, G.W. Irwin, Direct neural model reference adaptive control, IEE Proc. Cont. Theory Appl. 142 (1) (1995) 31–43.

[37] S.S. Ge, C.C. Huang, T. Zhang, Nonlinear adaptive control using neural networks and its application to CSTR systems, J. Process Cont. 9 (4) (1999) 313–323.